ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA DE TELECOMUNICACIÓN
UNIVERSIDAD POLITÉCNICA DE CARTAGENA

Proyecto Fin de Carrera

Puesta en marcha de los equipos de Nortel Networks Business Policy Switch 2000 y Contivity 400. Estudio práctico de sus capacidades de seguridad en redes de comunicaciones

AUTOR: Bienvenido Díaz Mateo
DIRECTOR: Cristina López Bravo
Enero / 2004

Autor	Bienvenido Díaz Mateo
E-mail del Autor	Bienve_diaz@wanadoo.es
Director(es)	Cristina López Bravo
E-mail del Director	cristina.lopez@upct.es
Codirector(es)	
Título del PFC	Puesta en marcha de los equipos de Nortel Networks Business Policy Switch 2000 y Contivity 400. Estudio práctico de sus capacidades de seguridad en redes de comunicaciones
Descriptores	Cortafuegos, VLAN, autenticación
Resúmen	
Titulación	Ingeniero Técnico de Telecomunicación
Intensificación	Telemática
Departamento	Departamento de Tecnologías de la información y las comunicaciones
Fecha de Presentación	Enero - 2004

Índice

Índice Figuras

Capítulo 1
Introducción

A lo largo de este proyecto se van a tratar varias cuestiones relacionadas con la seguridad en redes de comunicaciones, mediante el planteamiento de distintas problemáticas de seguridad y su posible solución, destinadas a comprobar el funcionamiento de los mecanismos de seguridad proporcionados por los equipos de *Nortel Networks*:

- *Contivity 400*
- *Business Policy Switch 2000*

Para poder hacer uso de las funciones de seguridad de ambos equipos, previamente se realizará la puesta en marcha de los mismos, proporcionándoles la configuración mínima necesaria para su incorporación a una red de comunicaciones. Posteriormente, una vez conocidos los dos problemas concretos a los que se pretende dar solución en este proyecto (descritos a continuación), se modificará dicha configuración básica, de manera que cumpla con los requisitos impuestos por cada problema.

Las funciones de seguridad que el *Contivity 400* proporciona son básicamente el uso de filtros para actuar como cortafuegos y su posible uso también como servidor *proxy*. En el capítulo 2 de este proyecto se describirán dichas características, centrándose en la capacidad del *Contivity 400* para actuar como cortafuegos. En dicho capítulo se plantea una problemática muy extendida en la actualidad, que está dando numerosos problemas a un elevado número de empresas, como es la vulnerabilidad de los servidores de acceso público. Debido a esta vulnerabilidad, la seguridad de los equipos de la red interna se ve comprometida, ya que cualquier atacante que consiga acceder a un servidor de acceso público, en una estructura de red normal, tendrá también acceso a cualquiera de los equipos de la red interna. Este problema nos va a permitir comprobar la funcionalidad del *Contivity 400* como cortafuegos. Para resolver este problema se han estudiado posibles arquitecturas de red, optando finalmente por el uso de una arquitectura *Screened Subnet* o DMZ. Dentro de esta arquitectura se hará funcionar al *Contivity 400* como cortafuegos, configurando una serie de filtros que serán aplicados a sus interfaces, cada una de las cuales conecta una subred de la arquitectura DMZ. De este modo que quedará correctamente probada la capacidad del Contivity 400 para actuar como cortafuegos. Todo el proceso de creación y posterior aplicación de filtros será explicado con detalle a lo largo del capítulo.

En cuanto al Business Policy Switch 2000 (BPS 2000), sus funciones de seguridad más relevantes son la implementación del protocolo EAPOL y la posibilidad de trabajar con un servidor de autenticación RADIUS. Ambas funciones serán usadas a lo largo del capítulo 3 para resolver el problema planteado en el mismo. Dicho problema está relacionado con la necesidad de proporcionar acceso a unos servicios telemáticos específicos a distintos grupos de usuario dentro de una organización. Debido a que, en la actualidad, la movilidad de los usuarios es grande y los servicios demandados por los mismos son muy diversos, se necesita dotar a la distribución de los grupos de una mayor flexibilidad que la que ofrece una estructura de red "*tradicional*", en la que el acceso a un servicio depende de a que roseta se conecte el usuario. Para ello, se usará la capacidad del BPS 2000 para crear Redes Virtuales

Locales (VLAN), asignando a cada grupo de usuarios a una VLAN específica, de modo que la composición de los grupos sea más flexible, dado que al trabajar con VLAN la distribución se hace a nivel lógico. También se hará uso de la capacidad del BPS 2000 de trabajar con el protocolo EAPOL, para proporcionar control de acceso a los distintos grupos. Dentro del protocolo EAPOL, para dotar de una mayor flexibilidad al proceso se usará la función de Asignación Dinámica de VLAN que proporciona el protocolo EAPOL y que es soportada por el BPS 2000. Será necesario, además de configurar la seguridad EAPOL y las distintas VLAN en el BPS 2000, instalar y configurar correctamente un servidor de autenticación RADIUS. Dicho servidor será el encargado de autenticar, a través de un identificador y una clave, cualquier acceso a los grupos de trabajo. El servidor RADIUS se usará también para proporcionar control de acceso, además de a los grupos de trabajo, a la interfaz de gestión del BPS 2000.

A pesar de que el formato de los capítulos 2 y 3 no se ajusta al formato convencional de una práctica, se espera que tanto el problema que plantea como su solución, se puedan utilizar como base para la elaboración de sendas prácticas para la asignatura “Seguridad en redes de comunicaciones” (5º curso de Ingeniero de Telecomunicación).

Capítulo 2
Cortafuegos

Este capítulo va a centrarse en el uso de cortafuegos o filtros con el objetivo de hacer más seguras las comunicaciones entre diferentes redes. En concreto, este capítulo trata la problemática de la vulnerabilidad de los servidores de acceso público, buscando una solución que permita que dichos servidores sigan siendo de acceso público, pero con unas condiciones de seguridad determinadas, para impedir el acceso al resto de equipos de una red corporativa una vez que han sido atacados con éxito los servidores. Es aquí donde aparece el término cortafuegos, que será el encargado de proteger el acceso a dichos servidores y a cualquier otra máquina de la red. La idea es aislar a los servidores de acceso público del resto de equipos situándolos en otra subred, pero al mismo tiempo permitir a las máquinas que lo necesiten comunicarse con ellos. Para ello se hará uso de un cortafuegos, configurado correctamente, que regule el tráfico entre las distintas redes, tanto privadas como públicas (Internet), y la red donde se encuentran los servidores de acceso público. Esta estructura de seguridad en la que se aísla a parte a los servidores de acceso público, separándolos del resto de máquinas de la red corporativa es lo que conoce como *Screened Subnet* o zona DMZ (*De-Militarized Zone*). Esta arquitectura será comentada con más detalle a lo largo de este capítulo, concretamente, en el apartado 2.1.4. Para regular y restringir el tráfico entre las redes externa, interna y la zona DMZ (zona donde se situarán los servidores de acceso público, tales como, por ejemplo, un servidor Web) el cortafuegos usará una serie de filtros, según las necesidades impuestas por la política de seguridad de la red. A lo largo de este capítulo se comentará extensamente en qué consisten dichos filtros así como su creación y posterior aplicación a las interfaces del cortafuegos.

El Contivity 400 de Nortel Networks ha sido el dispositivo elegido como cortafuegos. En este capítulo se describe, tanto en su instalación y puesta en marcha, como en su posterior configuración adaptada al cumplimiento de los requisitos de seguridad establecidos en el ejercicio planteado en este capítulo.

2.1 Introducción teórica

A continuación van a explicarse algunos de los conceptos usados posteriormente para la resolución del ejercicio propuesto en este capítulo tales como cortafuegos, *ipmasquerade* y *Screened Subnet*. La mayoría de ellos conceptos relacionados con la seguridad en redes de comunicaciones y que nos proporcionarán las características necesarias para resolver la problemática de seguridad planteada en este capítulo.

2.1.1 Cortafuegos

En este apartado se explicará brevemente en qué consiste un cortafuegos, así como sus diferentes tipos.

2.1.1.1 Definición

¿QUÉ ES UN CORTAFUEGOS?

Una definición genérica de lo que es un cortafuegos sería la siguiente:

Un cortafuegos es un sistema o grupo de sistemas que establecen una política de control de acceso entre dos redes.

Especificando un poco más tendríamos la siguiente definición:

Un cortafuegos se puede definir como un conjunto de reglas, aplicaciones y políticas que deben asegurar el acceso de los usuarios a los servicios de red, al tiempo que protegen nuestras redes de posibles ataques del exterior.

Los cortafuegos tienen las siguientes propiedades:

- Todo el tráfico de adentro hacia fuera, y viceversa debe pasar a través de él.
- Sólo el tráfico autorizado, definido por la política de seguridad, es autorizado para pasar por él.
- El sistema es realmente resistente a la penetración.

2.1.1.2 Tipos de cortafuegos

Los cortafuegos se pueden clasificar en función del nivel OSI en el que se implementa la política de seguridad definida para la red que se pretende proteger.

Cortafuegos como filtros

En primer lugar se encuentran los cortafuegos de nivel 3 de la capa OSI, es decir, de nivel de red o lo que es lo mismo, nivel IP en redes TCP/IP como Internet. Este tipo de cortafuegos pueden ser considerados como filtros de paquetes ya que lo que realizan, al fin y al cabo, es un filtrado de los intentos de conexión según las direcciones IP origen y destino, y puerto de origen o de destino de los paquetes IP.

Los encaminadores son un tipo especial de conmutadores que toman sus decisiones basándose en tablas de datos de encaminamiento. También pueden usar reglas, por medio de filtros, de modo que, por ejemplo, sólo tramas con una determinada dirección IP puedan pasar a través del encaminador. En este caso, los encaminadores se transforman en dispositivos de control de acceso o Cortafuegos.

Un ejemplo en el que sería útil un cortafuegos de este tipo, sería el caso de un servidor de Internet que bien solicita o bien suministra información a sistemas de

bases de datos distribuidas, en este caso, la conexión entre el servidor y la base de datos debería estar protegida o filtrada mediante un cortafuegos.

La mayoría de los Cortafuegos desempeñan algún tipo de filtrado de paquetes a través de un conmutador que es el que realiza la función de cortafuegos. El conmutador filtra paquetes implementando un conjunto de reglas que son las que definen la política del cortafuegos. Los filtros pueden ser definidos en base a criterios tales como:

- dirección IP fuente,
- dirección IP destino,
- puerto fuente TCP/UDP, y
- puerto destino TCP/UDP.

Mediante dichos filtros pueden bloquearse conexiones desde o a determinadas estaciones de trabajo, del mismo modo puede bloquearse también el acceso a puertos específicos. Un ejemplo de aplicación de estos filtros sería un caso en el que se desease bloquear el acceso a alguna de las máquinas consideradas como hostiles o indignas de confianza, o para el caso en el que se quiera bloquear el acceso a una determinada red desde todas las direcciones externas a dicha red, pero permitiendo alguna excepción como, por ejemplo, la conexión mediante SMTP, para poder recibir *mail* (para lo cual el filtro en cuestión especificaría como puerto permitido el puerto SMTP).

Mediante combinaciones de los sencillos criterios mencionados anteriormente pueden crearse complejas reglas de filtrado de múltiple funcionalidad que constituyan firmes políticas de control de acceso.

Cortafuegos como puerta de enlace

Se dice que un cortafuegos está trabajando como puerta de enlace (*gateway*) cuando controla el acceso desde fuera de una red hacia dentro y viceversa. Una puerta de enlace actúa como punto a través del cual se comunican dos redes. El tráfico de una red que se dirige al exterior de dicha red no se envía directamente a su destino, sino que es enviado a la pasarela. Dicha pasarela siguiendo una política de control de acceso determinada mediante una serie de filtros envía los paquetes a la red destino o a otra pasarela conectada a dicha red destino.

Este tipo de cortafuegos trabaja en el nivel 4 de OSI, es decir, a nivel de transporte o de TCP en redes TCP/IP. En este nivel ya se tiene en cuenta si los paquetes son de inicio de conexión o se corresponden con paquetes cuyas conexiones están ya establecidas. Por lo tanto, este tipo de cortafuegos ya trata con números de secuencias de paquetes TCP/IP.

Cortafuegos como proxy

Los cortafuegos que trabajan como *proxies* implementan la política de seguridad a nivel 7 de la capa OSI, es decir, a nivel de aplicación. Estos cortafuegos actúan a modo de *proxy* para las distintas aplicaciones que van a controlar.

Un servidor *proxy* (algunas veces se hace referencia a el con el nombre de puerta de enlace (*gateway*) o agente de transporte (*forwarder*)), es una aplicación que media en el tráfico que se produce entre una red protegida e Internet. Los *proxies* se

utilizan a menudo, como sustitutos de encaminadores controladores de tráfico, para prevenir el tráfico que pasa directamente entre las redes. Muchos *proxies* contienen identificadores de usuario auxiliares y soportan la autentificación de usuarios. Un *proxy* debe entender el protocolo de la aplicación que está siendo usada, aunque también pueden implementar protocolos específicos de seguridad (por ejemplo: un *proxy* FTP puede ser configurado para permitir FTP entrante y bloquear FTP saliente).

Los servidores *proxy*, son aplicaciones específicas. Un conjunto muy conocido de servidores *proxy* son los TIS Internet Cortafuegos Toolkit "FWTK", que incluyen *proxies* para Telnet, rlogin, FTP, X-Windows, HTTP/Web, y NNTP/Usenet news. SOCKS es un sistema *proxy* genérico que puede ser compilado en una aplicación cliente para hacerla trabajar a través de un cortafuegos.

Cortafuegos híbridos

En la práctica, muchos de los cortafuegos comerciales de hoy usan una combinación de estas técnicas. Por ejemplo, un producto que se originó como un cortafuegos filtrador de paquetes puede haber sido mejorado con filtrado inteligente a nivel de aplicación. Las aplicaciones *proxy* en áreas establecidas como *ftp* pueden agregar una inspección de filtrado base en su esquema.

2.1.1.3 Inspección de paquetes

Algunos cortafuegos de Internet combinan el filtrado de paquetes y el enfoque de aplicaciones de puerta de enlace, usando un filtrado de paquetes o un encaminador *hardware* para controlar los niveles bajos de comunicación, y una puerta de enlace para habilitar aplicaciones. Esto puede crear un alto grado de control de acceso. Como siempre, esta adaptación puede limitar en transparencia, flexibilidad y conectividad, y puede también dar una mayor dificultad en términos de configuración, manejo y especialización.

Una idea que gana aceptación es la inspección de paquetes que considera tanto su contenido como sus direcciones. Los cortafuegos de este tipo emplean una inspección modular, aplicable a todos los protocolos que comprenden los datos de los paquetes destinados desde el nivel de red hasta el nivel de aplicación. Esta estrategia puede proveer seguridad dependiente del contexto para complejas aplicaciones y puede ser más efectiva que las tecnologías que sólo tienen acceso a los datos en ciertos niveles. Por ejemplo, las aplicaciones de puerta de enlace sólo acceden a los datos de nivel aplicación, los encaminadores tienen acceso sólo a niveles bajos, el enfoque de la inspección de paquetes integra toda la información reunida de todos los niveles en un simple punto de inspección.

El filtrado inteligente puede combinarse efectivamente con la habilidad del rastreo de la sesión de red. Para usar la información acerca del inicio y fin de la sesión en la decisión de filtrado. Esto es conocido como filtrado por sesión (*sesión filtering*). Los filtros usan reglas inteligentes, así aumenta el proceso de filtrado y controlando el rastreo de sesiones de la red que controla los paquetes individuales.

Una sesión de red contiene paquetes que van en dos direcciones, así que sin una sesión de filtrado cada sesión requiere dos reglas de filtrado de paquetes. La primera controla los paquetes que van desde el equipo origen hasta el equipo destino.

Este enfoque ofrece ventajas considerables, desde los sitios que comúnmente tratan los paquetes originados afuera del cortafuegos de manera diferente que los paquetes que regresan desde una conexión autorizada afuera.

2.1.2 Ipmasquerade

Un concepto que está íntimamente ligado al filtrado es *ipmasquerade*. Supongamos que tenemos un *proxy* tradicional con una dirección IP pública y una red privada tras él con direcciones privadas (192.168.0.0). En este caso, habrá que decirle a las aplicaciones que se ejecuten en los equipos de la red privada que tienen que conectarse a través de un *proxy*, especificando su dirección y puerto. Las aplicaciones establecerán una conexión con el *proxy* cuando deseen un servicio remoto.

En el caso de usar *masquerade*, tenemos una puerta que implementa *masquerade* con una dirección IP pública y una red privada detrás. En este caso, los equipos de la red privada no saben que usarán *masquerade*, simplemente se configuran para que las conexiones que salgan al exterior atraviesen la puerta (sería el encaminador por defecto). Cuando una aplicación necesita un servicio externo, intenta establecer una conexión como si estuviera directamente conectada al exterior y envía sus paquetes al encaminador por defecto. Al llegar el paquete a la puerta, se cambia la dirección origen por la de la puerta, se le asigna un puerto y se envía al exterior. Cuando llegue la respuesta, se cambia la dirección de destino por la del equipo y puerto original y se envía a la red privada. Esto permite usar redes privadas sin tener que configurar las aplicaciones para utilizar un *proxy*.

En el caso del ejercicio planteado en este capítulo, los PC pertenecientes a la red interna harán uso de *ipmasquerade* para tener acceso al exterior, mediante un servidor *proxy* con una dirección pública.

Como se puede observar, en ambos casos se proporciona un servicio *NAT (Network Adress Translation)* en el que se sustituyen las conexiones originales por otras, pero de diferente forma. El conmutador *Contivity 400* hará uso del servicio NAT para la realización del ejercicio propuesto en este capítulo.

Un *proxy*, además de sustituir las conexiones, puede filtrarlas, entonces es cuando se tiene un cortafuegos. Lo mismo ocurre con *ipmasquerade*, cuando se aplican reglas de filtrado, se obtiene un cortafuegos.

Todo esto es válido para redes privadas, que no serán accesibles desde el exterior porque no se puede saber la dirección IP de los equipos (desde el punto de vista externo, sólo se puede llegar a la puerta que tiene la dirección pública).

En el caso de una red pública normal, en el que cada equipo tiene una dirección IP pública, el encaminador de salida puede proporcionar servicios de Cortafuegos cuando se configura para que establezca reglas de filtrado de conexiones (en función del contenido o de otros parámetros).

2.1.3 Seguridad en la arquitectura de nuestra red

A continuación se verán algunos ejemplos de arquitecturas de red que ofrecen servicios de seguridad.

En la actualidad, la arquitectura más usada para ofrecer servicios a través de una red es la arquitectura de tres capas (Three-Tier Architecture).

En esta arquitectura el cliente (1ª capa) se comunica con un servidor de aplicaciones (capa intermedia) de cualquier tipo como por ejemplo un servidor Web, un servidor de objetos, etc, a través del protocolo adecuado como HTTP o CORBA. El servidor de aplicaciones procesa la petición y accede a los recursos necesarios (3ª capa) que pueden ser una base de datos, una aplicación propietaria, etc. El protocolo usado para acceder a la tercera capa no tiene porqué ser igual al usado por el cliente para conectarse con el servidor. Posteriormente se envía la respuesta al cliente.

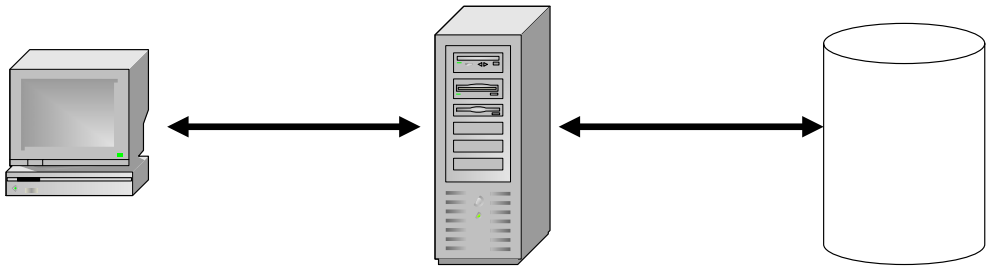

Figura -2.1- Arquitectura Three-Tier

Un ejemplo de esta arquitectura es un servidor HTTP que procesa las peticiones mediante un *servlet*, el cual accede a una base de datos a través del protocolo adecuado. En un servidor de aplicaciones suelen convivir diversas tecnologías que cooperan entre ellas para proporcionar los servicios ofertados, como por ejemplo, servidores Web, *servlets*, *scripts* CGI, PHP, servidores de objetos distribuidos, etc. El hecho de que esas tecnologías interactúen entre ellas suele crear agujeros de seguridad. El administrador tiene que revisar continuamente el entorno del servidor asegurándose de que está adecuadamente configurado, el acceso está controlado, y sólo están presentes los servicios necesarios.

Una forma habitual de controlar el acceso es instalar un cortafuegos delante del servidor.

Si el cortafuegos está bien configurado puede ser un método eficaz de protección. Pero imagine que hay algún detalle que se le ha escapado o que se añaden nuevos servicios a la red, es posible que exista algún agujero. La segunda y tercera capa (que normalmente es la más importante pues es la que contiene la información crítica) están físicamente conectadas. Normalmente gastando sólo un poco más se pueden separar físicamente las redes, añadiendo un segundo interfaz al servidor.

Una solución más costosa pero más segura es incluir un segundo cortafuegos al modelo para aislar los recursos y nuestras subredes del servidor.

Una solución intermedia es considerar el propio tipo de red. Por ejemplo, utilizar otros protocolos para comunicar los recursos con el servidor, por ejemplo SNA, o usar

un pequeño programa de comunicaciones sobre un enlace serie dedicado. Muchos ataques sólo son posibles usando TCP/IP.

Sin embargo, no hay que olvidar que si el atacante consigue tomar el control del servidor de aplicaciones, probablemente tendrá control sobre los programas de comunicaciones.

2.1.4 Arquitectura *Screened Subnet*

Esta arquitectura merece una mención especial dado que es la arquitectura que va a ser usada para la resolución del ejercicio que se plantea en este capítulo.

La arquitectura *Screened Subnet*, también conocida como red perimétrica o *De-Militarized Zone* (DMZ) es, con diferencia, la más utilizada e implantada hoy en día. La arquitectura DMZ añade un nivel de seguridad en las arquitecturas de cortafuegos situando una subred (DMZ) entre las redes externa e interna, de forma que se consiguen reducir los efectos de un ataque exitoso a algún servidor de acceso público, como por ejemplo, un servidor Web. En los modelos anteriores, toda la seguridad se centraba en el encaminador, de forma que si la seguridad del mismo se veía comprometida, la amenaza se extendía automáticamente al resto de la red. Como los servidores de acceso público, tales como un servidor de correo o un servidor Web, es un objetivo interesante para muchos piratas, la arquitectura DMZ intenta aislarla en una red perimétrica de forma que un intruso que accede a esta máquina no consiga un acceso total a la subred protegida.

Screened subnet es la arquitectura más segura, pero también la más compleja; se utilizan dos *encaminadores*, denominados exterior e interior, conectados ambos a la red perimétrica, como puede apreciarse en la figura 1. En esta red perimétrica, que constituye el sistema cortafuegos, se incluye un Servidor Web y también se podrían incluir sistemas que requieran un acceso controlado, como baterías de módems o el servidor de correo, que serán los únicos elementos visibles desde fuera de nuestra red. El *encaminador* exterior tiene como misión bloquear el tráfico no deseado en ambos sentidos (hacia la red perimétrica y hacia la red externa), mientras que el interior hace lo mismo pero con el tráfico entre la red interna y la perimétrica: así, un atacante habría de romper la seguridad de ambos *encaminadores* para acceder a la red protegida; incluso es posible implementar una zona desmilitarizada con un único *encaminador* que posea tres o más interfaces de red (que es la opción que se va a utilizar en este proyecto), pero en este caso, si se compromete este único elemento se rompe toda nuestra seguridad, frente al caso general en que hay que comprometer ambos, tanto el externo como el interno. También podemos, si necesitamos mayores niveles de seguridad, definir varias redes perimétricas en serie, situando los servicios que requieran de menor fiabilidad en las redes más externas: así, el atacante habrá de saltar por todas y cada una de ellas para acceder a nuestros equipos; evidentemente, si en cada red perimétrica se siguen las mismas reglas de filtrado, niveles adicionales no proporcionan mayor seguridad.

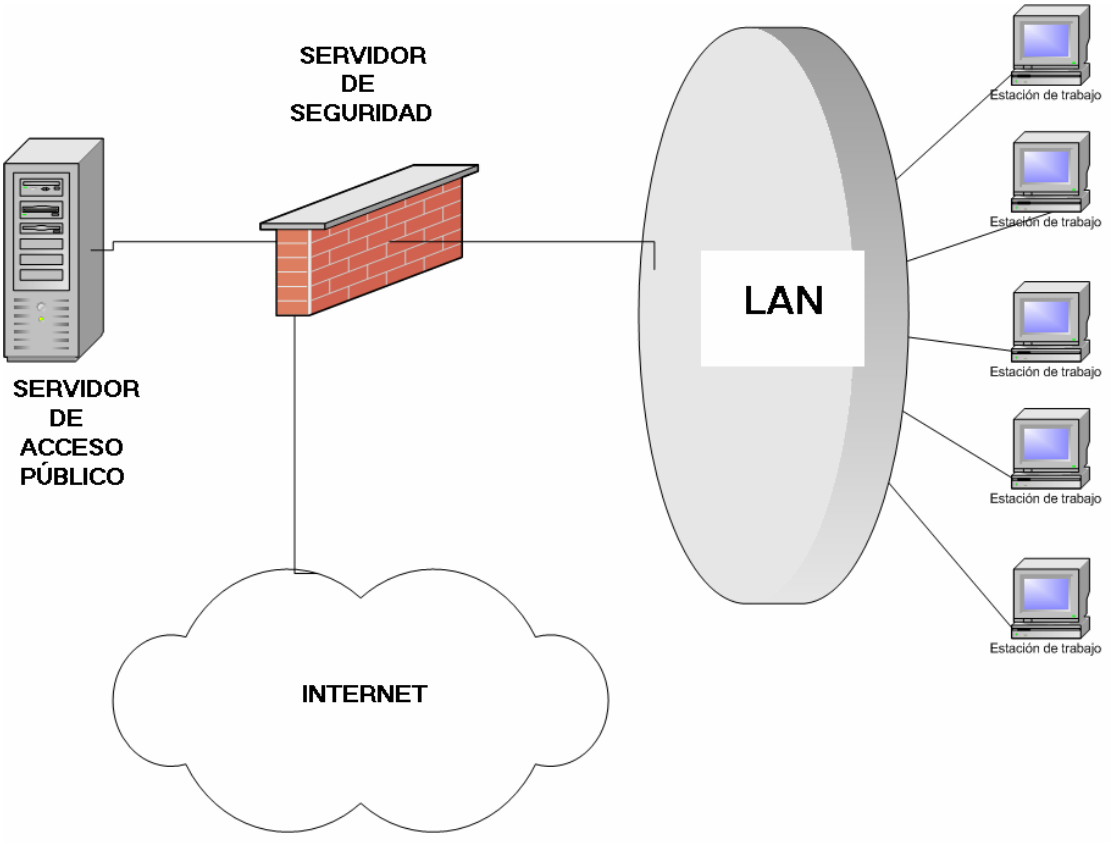

Figura -2.2- Arquitectura *Screened Subnet*

Esta arquitectura de cortafuegos elimina los puntos únicos de fallo presentes en las anteriores: antes de llegar al Servidor Web (que es un sistema vulnerable) un atacante ha de saltarse las medidas de seguridad impuestas por el encaminador externo. Si lo consigue, como hemos aislado el servidor Web en una subred estamos reduciendo el impacto de un atacante que logre controlarlo, ya que antes de llegar a la red interna ha de comprometer también al segundo encaminador. Por supuesto, en cualquiera de los tres casos (compromiso del encaminador externo, del servidor Web, o del encaminador interno) las actividades de un pirata pueden violar nuestra seguridad, pero de forma parcial: por ejemplo, simplemente accediendo al primer encaminador puede aislar toda nuestra organización del exterior, creando un problema, en cuanto a servicios se refiere, importante. Pero esto suele ser menos grave que si lograra acceso a la red protegida.

Aunque pueden darse problemas, sobre todo por errores en la configuración de los encaminadores encargados de realizar el filtrado, cabe destacar de nuevo que la arquitectura DMZ es la más indicada para proteger una red privada de accesos externos.

2.2 Desarrollo del ejercicio “Seguridad en la red mediante cortafuegos”

En este apartado se explicará cuales son las posibilidades que ofrece la unidad Contivity para actuar como cortafuegos así como la configuración a realizar por parte del usuario de la de dicha unidad para la realización correcta del ejercicio.

2.2.1 Características de *Contivity 400* como cortafuegos

El *Contivity 400* dispone de funcionalidades que le permiten actuar eficientemente como un cortafuegos, bien sea en una estructura normal o en una estructura DMZ (que es la que se planteará más tarde en el ejercicio), ya que posee hasta tres interfaces de red (de tipo *Ethernet*).

Para realizar las funciones de cortafuegos, el Contivity 400 se basa en el filtrado de paquetes.

Cada vez que se crea un filtro, éste se añade a la lista de filtros del *Contivity 400* y puede aplicarse a cualquiera de las interfaces de dos formas:

- Como **filtro de entrada** de una determinada interfaz: de este modo aplicamos el filtro a los paquetes que son recibidos por la interfaz en cuestión.
- Como **filtro de salida**: en este caso el filtro se aplica a los paquetes justo antes de ser transmitidos por la interfaz.

Un mismo filtro puede ser aplicado a varias interfaces o sobre una misma, haciendo tanto de filtro de entrada como de filtro de salida.

Los paquetes procesados por un determinado filtro llevan a cabo el siguiente proceso: recorren la lista de reglas desde arriba hacia abajo, y en caso de que no haya ninguna regla aplicable a dicho paquete dentro de esa lista de reglas, el *Contivity 400* está configurado por defecto para descartar ese tipo de paquetes. En caso de que sí cumplan las especificaciones de una determinada regla se procesan de acuerdo a la acción determinada para dicha regla.

Un filtro consiste en una lista de reglas o políticas. A la hora de definir las reglas que compondrán cada filtro el *Contivity 400* ofrece una flexibilidad considerable para dicho fin, dichas reglas se pueden definir en función de los siguientes parámetros:

Tipo de protocolo: Se especifica el protocolo al que deben pertenecer los paquetes para ser tratados por esta regla. El *Contivity 400* permite identificar los paquetes de 4 protocolos diferentes:

- *IP* (*Internet Protocol*).
- *TCP* (*Transmisión Control Protocol*). En el caso del protocolo TCP se ofrece la posibilidad de poder activar una opción que permite relacionar los paquetes pertenecientes a conexiones estabilizadas. Esto suele ser utilizado para permitir paquetes de estaciones con sesiones de trabajo establecidas y a su vez prevenir el acceso a los servidores.
- *UDP* (*User Datagram Protocol*).
- *ICMP* (*Internet Control Message Protocol*).

Fuente: Respecto a la fuente el *Contivity 400* permite especificar los siguientes parámetros:

- *Address*: Aquí se indica la dirección fuente de los paquetes a los que se le aplicará la regla.
- *Bits*: Mediante este número se indica el número de bits correspondientes a la máscara de subred de la dirección fuente. El valor por defecto es 32 (valor que tomará si dejamos en blanco este apartado), lo que quiere decir que se toman sólo aquellos paquetes cuya dirección IP coincida exactamente con la dirección IP que hemos especificado. Sin embargo, escribiendo 24 en esta casilla, si por ejemplo se ha especificado la dirección *192.168.1.1* se toman como válidas todas aquellas direcciones que empiecen por *192.168.1*, es decir, todas las direcciones pertenecientes a la misma subred.
- *Port*: Especificamos el puerto fuente que debe tener el paquete para que la regla le sea aplicable.
- *Ending Port*: Este apartado sirve para especificar un rango de puertos, el cual estaría definido entre el puerto especificado en *Port* y el puerto especificado en *Ending Port.*

Destino: El *Contivity 400* ofrece las mismas posibilidades de configuración para el destino que para la fuente, por lo tanto todo lo explicado anteriormente para la fuente es aplicable al destino.

Una vez que se ha realizado el filtrado mediante los campos anteriormente comentados, las acciones a ejecutar con los paquetes que ofrece el *Contivity 400* son las siguientes:

- *Allow*: permitir el paso de los paquetes que cumplan los requisitos.
- *Deny*: denegar el paso de dichos paquetes.
- *L4conmutador*: enviar los paquetes a través del servidor *proxy*.
- *NAT*: Envía los paquetes para traducción de direcciones, ésta será realizada en la máquina destino.

Las reglas que componen los filtros pueden ordenarse según las preferencias de cada usuario seleccionando una determinada regla de la lista de reglas que componen el filtro y haciendo uso de los cursores para situarla en una posición más avanzada o más retrasada en la lista.

Además de los filtros asociados a las interfaces para completar las funciones en lo que a restricción o seguridad se refiere, cabe también mencionar que el Contivity puede actuar como servidor Web (*proxy*), bloqueando las *co"OK"ies* y restringiendo el acceso a sitios Web, todas estas características configuradas por el usuario. Esto se realiza mediante el acceso vía Web, el cual se realiza desde un navegador Web escribiendo la dirección IP de cualquiera de las interfaces del *Contivity 400* que estén configuradas, cada una con su dirección IP correspondiente, y pulsando *Enter*. De este modo, se accederá a una Web cuyo aspecto es el que se muestra en la figura 28, esta Web tiene 3 zonas principales:

- **HOME**: Es la zona a la cual se accede por defecto al entrar a la Web, contiene datos básicos sobre nuestra unidad *Contivity 400* tales como el número de serie y la versión de la misma.
- **ADMIN**: Zona desde la cual se puede administrar la mayoría de propiedades del conmutador (excepto la Web Caché que tiene su apartado propio).

- **WEB CACHE**:Esta es la zona que más interesante de las tres, ya que desde aquí es posible configurar la unidad *Contivity 400* para que actúe como un Servidor *Proxy* a través del cual las máquinas puedan acceder a Internet mediante una única conexión y además realizando funciones de filtrado. Las tres funciones o beneficios principales que nos puede producir *Contivity 400* actuando como servidor *proxy* son:

    - Aumento de la eficiencia: reduciendo el tiempo de acceso y optimizando el ancho de banda usando los contenidos de la caché para entradas compartidas.
    - Manejo de *co"OK"ies*: con lo que permite aumentar la seguridad así como el rendimiento de la caché.
    - Control sobre el acceso a sitios Web: pudiendo prohibir el acceso a determinados sitios Web, lo cual puede ser útil tanto para uso doméstico (protección infantil) como para uso empresarial (evitar recreo de los empleados).

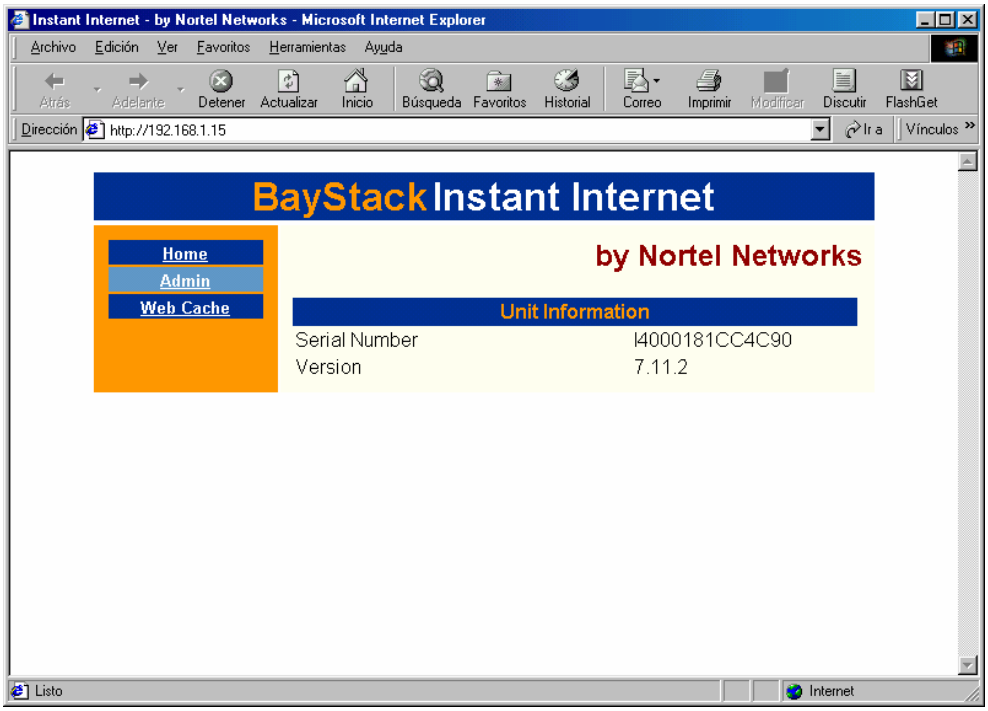

Figura -2.3- Ventana *Home* de la interfaz Web de administración

Para más información sobre la configuración del *Contivity 400* como Servidor *Proxy* referirse al documento "*Using Web management for Contivity 400*".

2.2.2 Planteamiento

Una vez que han sido vistas las características que ofrece el *Contivity 400* en su función como Cortafuegos, va a plantearse un ejercicio en cuya resolución se mostrará la funcionalidad de dichas características.

La situación es la siguiente: una empresa desea dotar de mayor seguridad a su estructura de red. En la red de la empresa hay equipos vulnerables, debido a que son de acceso público, como pueden ser los servidores Web o servidores de correo al mismo tiempo que también hay una red interna cuyos datos son privados y no se desea que sean accesibles desde ninguna localización exterior no autorizada. El problema está en que al estar estos equipos juntos en una misma red, cualquier atacante que consiga hacerse con el control de cualquiera de los servidores de acceso público tendrá también acceso a los equipos de la red interna. Para solucionar este problema, en este proyecto va a usarse lo que se denomina como arquitectura *Screened Subnet* o *Zona DMZ* (*De-Militarized Zone*), que ha sido comentada en el apartado 2.1.4 de este mismo capítulo. Por lo tanto, para aumentar la seguridad de la red de la empresa, lo que se hará es separar los servidores de acceso público de la red interna de la empresa, de modo que los servidores de acceso público queden encuadrados en una subred, que será lo que se denomine como *Zona DMZ*. El resto del esquema de la arquitectura se completará con la zona externa y la zona interna, ésta última será la que corresponde a la red interna de la empresa. En esta arquitectura de red, un atacante que consiga hacerse con el control de cualquiera de los servidores de acceso público no tendrá también acceso a las máquinas de la red interna, puesto que para ello deberá romper otra barrera más de seguridad, que consistirá en otra interfaz de la unidad *Contivity 400* con sus correspondientes filtros asociados, para poder acceder a la zona interna de la arquitectura de seguridad.

La resolución de este ejercicio consiste en configurar las tres interfaces de la unidad *Contivity 400* y crear una serie de filtros que serán aplicados a las mismas de modo que se regule el acceso entre las diferentes zonas actuando como Cortafuegos, de tal forma que la arquitectura resulte lo más segura posible.

El esquema de la arquitectura de red que se utiliza para resolver el ejercicio es el siguiente:

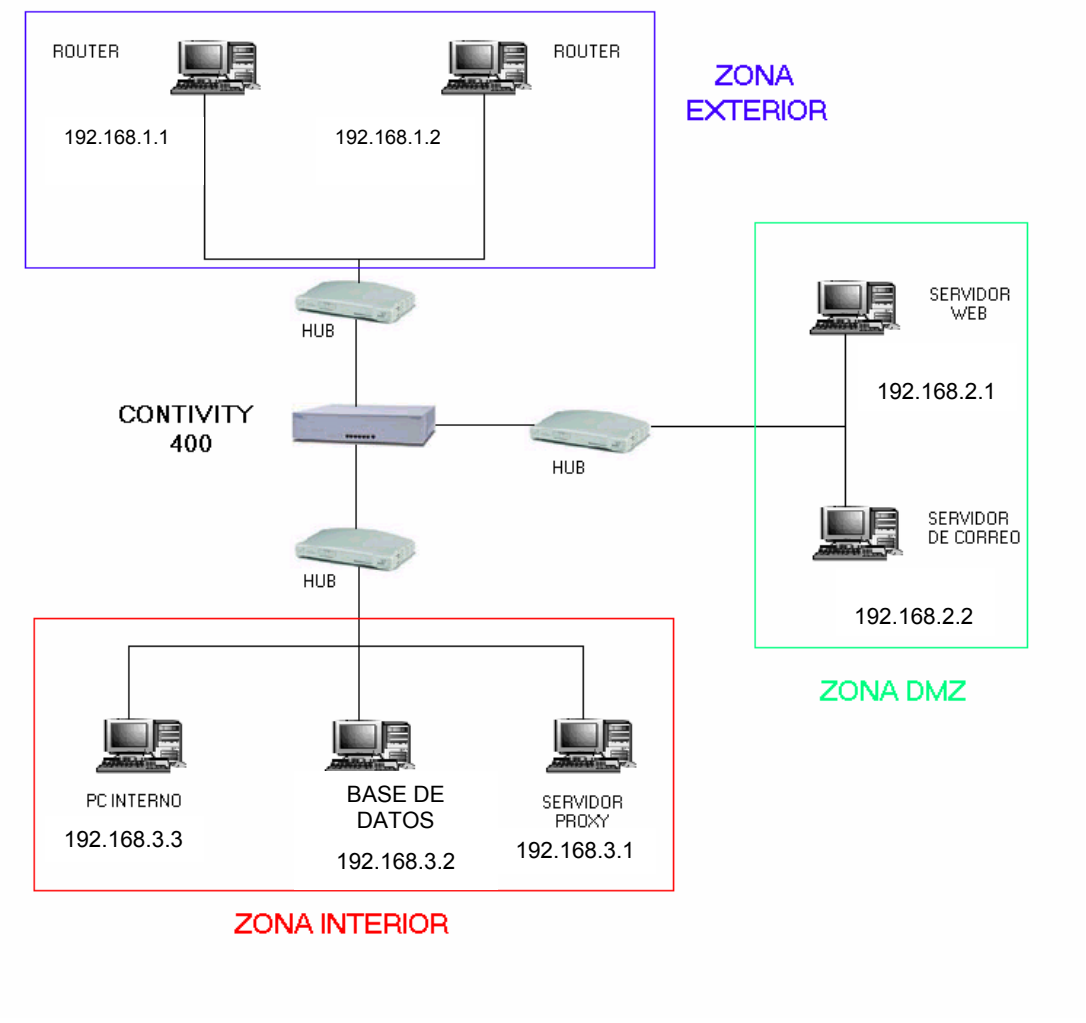

Figura -2.4- Esquema de red del ejercicio planteado

En dicho esquema se puede observar como existen 3 zonas bien diferenciadas:

- **Red Externa**: Zona exterior, donde se encuentran los 2 encaminadores que proporcionan el acceso a Internet, ésta última formaría parte también de esta zona.
- **Red Interna**: Esta zona representaría la red privada, en la cual, como es lógico se desea que haya la máxima seguridad posible, aislándola de la zona exterior para así protegerla de posibles ataques.
- La **salida a Internet** de todos los equipos de la red interna se realizará a través del servidor *proxy* por cualquiera de los encaminadores.
- **Zona DMZ**: En esta zona es donde estarán situados todos los servidores que se desea que sean de acceso público, tanto desde Internet como desde otras redes externas, en nuestro caso el servidor Web y el servidor de correo.

Para cumplir las condiciones de seguridad requeridas la configuración a realizar es la siguiente:

- La única máquina que puede salir al exterior es el servidor *Proxy*.
- Todas las maquinas de la red externa y de la red interna pueden acceder a la zona DMZ, pero sólo al servidor de correo mediante NAT de los puertos IMAP3, POP3 y SMTP, y al servidor Web mediante NAT de los puertos HTTP y HTTPS.
- El servidor Web debe comunicarse con la base de datos de la red interna, pero sólo mediante los puertos necesarios (En nuestro caso el puerto 1521, que es puerto por defecto de la base de datos *Oracle*).
- En la red interna se usará direccionamiento privado y a su vez direccionamiento NAT (*Network Address Translation*).
-

Para realizar esta configuración se debe crear una serie de filtros que cumplan dichas especificaciones y aplicarlos a las interfaces correspondientes del Contivity, teniendo en cuenta que la distribución de las interfaces es la siguiente:

- **Interfaz 1**: comunica al *Contivity 400* con la Red Externa y viceversa.
- **Interfaz 2**: comunica al *Contivity 400* con la Zona DMZ y viceversa.
- **Interfaz 3**: se hace cargo de la comunicación entre el *Contivity 400* y la Red Interna en ambos sentidos.

2.2.3 Resolución del ejercicio propuesto

Una vez establecidos los requisitos a cumplir, comienza la configuración específica de la unidad *Contivity 400* para cumplir dichos requisitos.

2.2.3.1 Configuración inicial *Contivity 400*

En este apartado va a explicarse como configurar el conmutador *Contivity 400* de *Nortel Networks*, partiendo desde el primer contacto con el conmutador, hasta la exploración de sus opciones más avanzadas de configuración.

Puesta en marcha

En primer lugar se conecta el conmutador a la red, a la cual pertenece el equipo desde donde va a configurarse el conmutador, haciendo uso de una de las tres interfaces que posee para la conexión a redes de área local, todas ellas deben estar conectadas a la red desde donde se desea configurar el conmutador, para no tener problema alguno durante su configuración.

El paso siguiente será encender el conmutador mediante el interruptor situado en su parte posterior. Pero antes de activar dicho interruptor debe comprobarse la posición de los 8 interruptores de configuración situados en la parte posterior del conmutador.

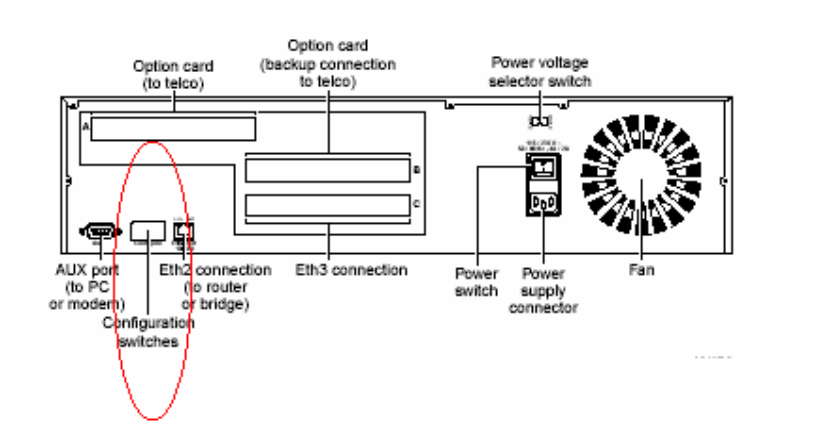

Figura -2.5- Frontal trasero *Contivity 400*

Los interruptores tienen dos posiciones posibles:

Abajo → ON

Arriba → OFF

Deben estar todos situados en la posición de OFF (arriba), lo que indica que el conmutador trabaja en modo normal, es decir, que no aplica ningún tipo de función especial, ni modifica ningún parámetro ya existente tales como perfiles de usuario o clave. En la siguiente figura se muestra como deben quedar configurados los interruptores:

	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
OFF	*	*	*	*	*	*	*	*
ON								

Figura -2.6- Combinación de interruptores para trabajo en modo normal

Para asegurarse de que va a partirse de la configuración por defecto, la que viene de fábrica, antes de encender el conmutador se sitúan los interruptores tal y como se muestra en la siguiente figura:

	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
OFF				*				*
ON	*	*	*		*	*	*	

Figura -2.7- Combinación de interruptores para aplicar configuración de fábrica

Una vez hecho esto, se enciende el conmutador y se espera hasta que los LEDs 1-8 y el LED POWER brillen en color naranja. Cuando esto ocurra, se apaga el conmutador. Vuelven a colocarse ahora los interruptores de configuración para operar en modo normal, tal y como se ha explicado anteriormente. A continuación, se enciende el conmutador y se espera hasta que el LED 2 brille en naranja, hecho que indica que el conmutador esta preparado para ser configurado.

Para asegurarse de que la secuencia de arranque ha sido realizada sin ningún tipo de problema, debe comprobarse también que el LED POWER, de la parte frontal del conmutador, está encendido con una luz verde fija, lo que indica que el conmutador tiene energía eléctrica y está encendido, y que el LED 1 situado en el panel frontal del conmutador este parpadeando con color verde, lo que indicará que el conmutador está funcionando con normalidad.

Instalación del *software* de *Nortel Networks*

Ahora es el momento de instalar el *software* que acompaña a la unidad Contivity. Dentro del CD que acompaña al conmutador, se ofrecen las siguientes opciones mediante un menú de autoarranque (suponiendo que está activada dicha opción en el equipo desde donde se va a configurar la unidad *Contivity 400*, si no basta con ejecutar el fichero *autorun.exe* que se encuentra en el CD para ver el menú de autoarranque que se muestra en la figura 5):

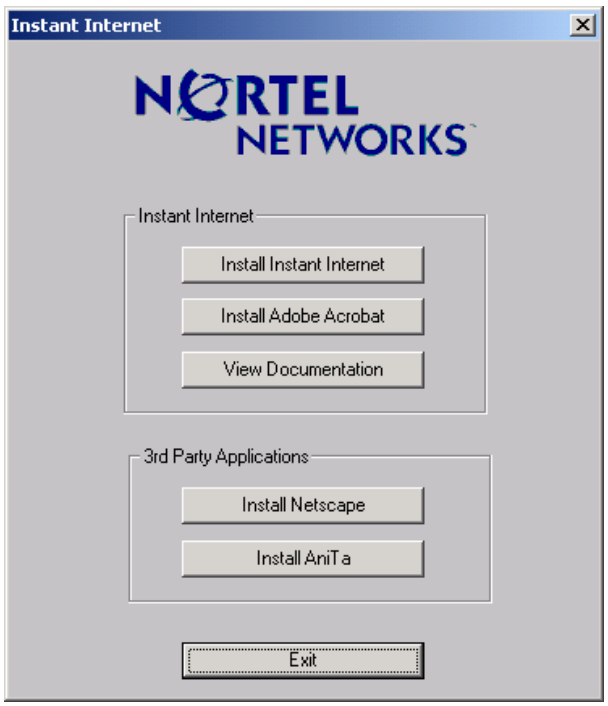

Figura -2.8- Menú de autoarranque del *software* de *Nortel Networks* que acompaña a la unidad *Contivity 400*

Antes de comenzar a instalar el programa hay que asegurarse de que el LED 2 está encendido y de color naranja, una vez que esto sucede puede comenzarse la instalación.

Tras realizar el programa la copia de una serie de archivos necesarios para la instalación se abre el cuadro de diálogo "*Enter Unit's IP Address*".

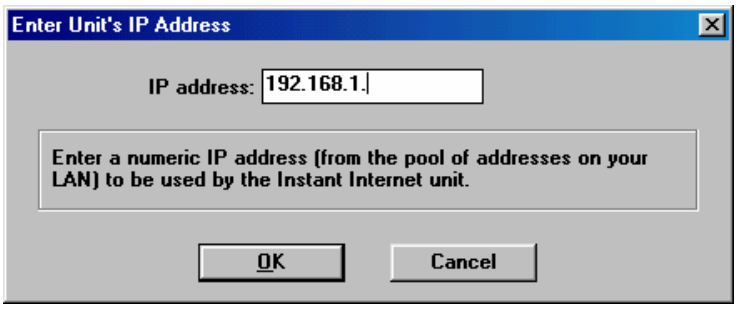

Figura -2.9- Cuadro de diálogo "*Enter Unit's IP Address*"

El programa detecta automáticamente la dirección de la red en la que se encuentra el equipo en el que se está instalando el *software*, siempre y cuando dicha red esté trabajando sobre TCP/IP. El usuario debe completar, dicha dirección de red, con la dirección de *host* que desee, asegurándose de que no coincida con una dirección ya asignada a cualquier otro equipo de la red. Una vez hecho esto se nos muestra el cuadro de diálogo *"DHCP server confirmation",*

Figura -2.10- Cuadro de diálogo para la elección de servidor DHCP

Si va a trabajarse con el conmutador funcionando como un servidor DHCP el cual va a ir asignando dinámicamente direcciones IP a los distintos equipos de la red, se elige la opción "*Yes*", en caso de que se trabaje con direcciones IP estáticas se elige la opción "*No*". En nuestro caso no va a trabajarse con ningún servidor DHCP por lo que elegimos la segunda opción. Tras este paso nos encontramos con el cuadro de diálogo "*Registration Information*".

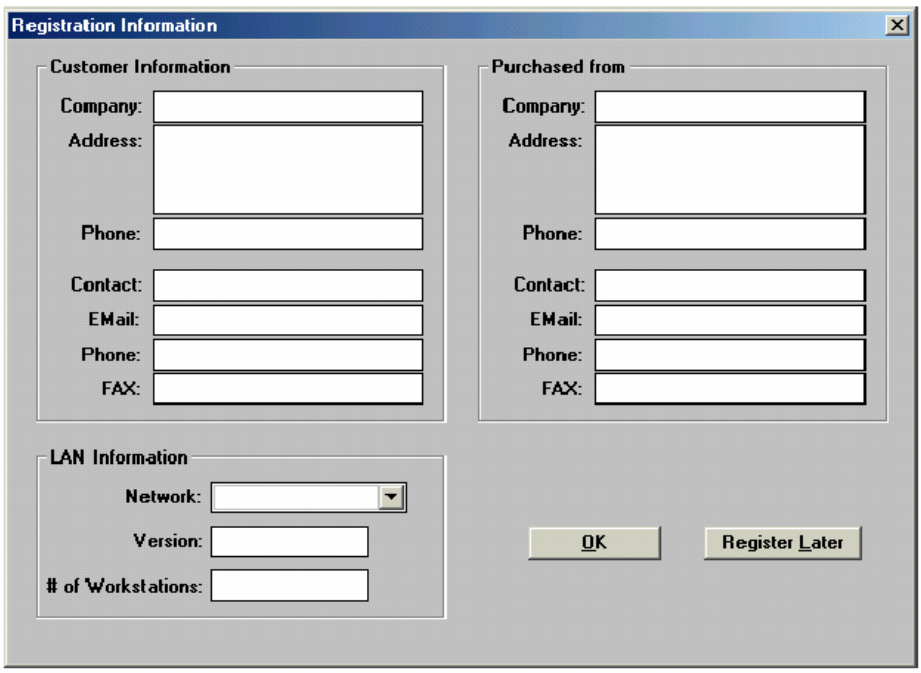

Figura -2.11- Cuadro de diálogo "*Registration Information*"

En esta ventana se ofrece al usuario la oportunidad de registrar el producto, de tal forma que *Nortel Networks* notifique a éste cualquier novedad o promoción que surja en su entorno, Este apartado no es imprescindible para seguir trabajando con el conmutador. En caso de registrarlo, cuando hayan sido rellenados todos los datos, al pulsar *"OK"* dicha información será directamente enviada a la empresa *Nortel Networks* la primera vez que se use el conmutador para la conexión a Internet.

En caso de que el usuario no quiera registrarse, basta con hacer click sobre "*Register Later*" y aparece la ventana "*Enter Name and Password*".

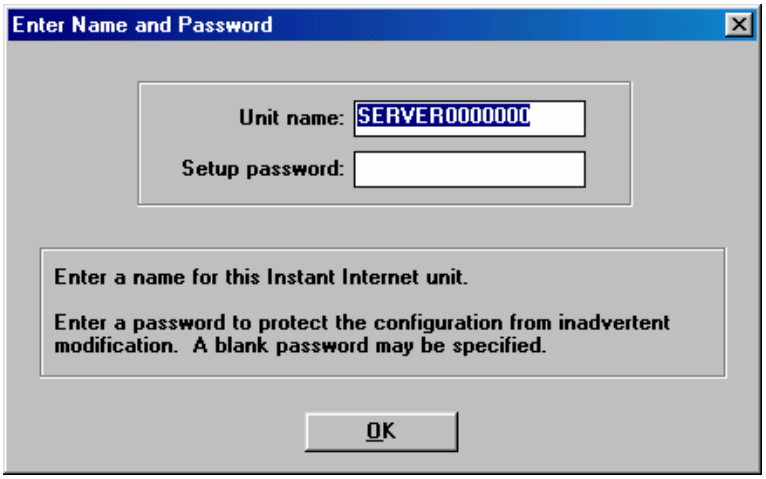

Figura -2.12- Cuadro de diálogo "*Enter Name and Password*"

En esta ventana se ofrece la opción de dotar a la unidad *Contivity 400* de un nombre, de una longitud máxima de 13 caracteres que podrán ser números, letras y símbolos, pero nunca espacios, y de una clave. En caso de no rellenar la casilla de la clave, la maquina podría ser accedida y configurada por cualquier máquina sin ningún tipo de autentificación ni contraseña. De este hecho se advierte al usuario mediante la siguiente ventana:

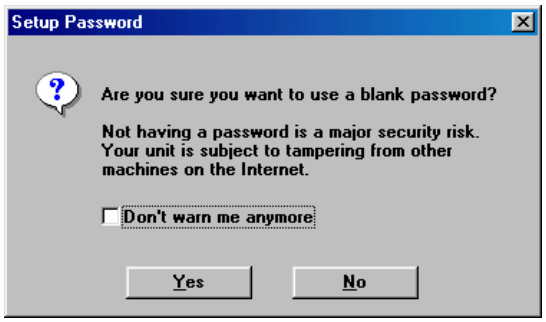

Figura -2.13- Cuadro de diálogo que advierte al usuario de la ausencia de una clave que proteja la unidad *Contivity 400*

De todos modos este apartado puede ser cambiado posteriormente en la opción *Password* que se encuentra en la ventana *"Setup"* del programa, donde puede dotarse de una clave a la unidad o cambiar el que ya tiene asignado.

Por último aparecerá la ventana para configurar los datos del proveedor de servicios, donde se configuran los parámetros relacionados con el mismo: número de teléfono, usuario, etc.

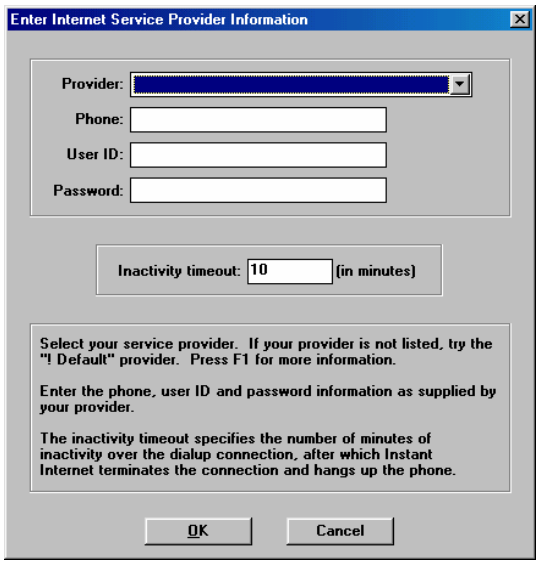

Figura -2.14- Cuadro de diálogo para la configuración de los parámetros referentes al proveedor de servicios

Una vez rellenados los datos correspondientes al ISP (Internet Services Provider), podemos elegir entre introducir un identificador de usuario (ID) o no, en caso de que se dejen estas casillas sin rellenar el programa indicará si quiere crearse un usuario (mediante su identificador de usuario) mediante el siguiente cuadro de diálogo:

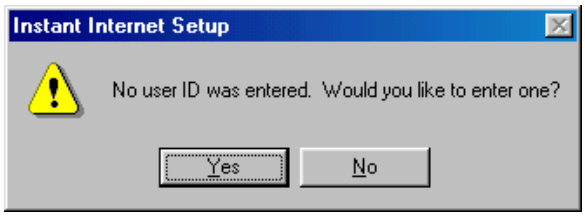

Figura -2.15- Cuadro de diálogo que advierte al usuario de la ausencia de un identificador de usuario, dándole la oportunidad de introducirlo

Si no quiere introducirse ningún identificador de usuario se pulsa *No* y aparece la caja de diálogo en la que se introduce la información acerca de la conexión ISDN (*Integral Services Digitals Networks*), dicho cuadro de diálogo tiene el siguiente aspecto:

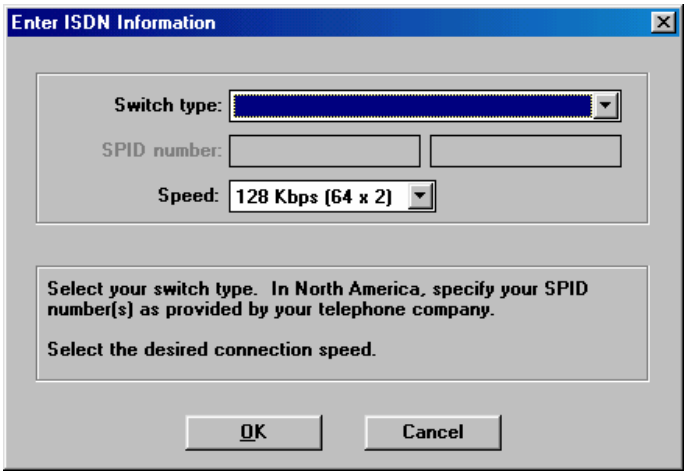

Figura -2.16- Cuadro de diálogo para la configuración de la interfaz ISDN

Como vemos puede elegirse entre distintos tipos de conmutador, y el tipo de acceso. Por ejemplo, el de la figura se correspondería con la velocidad de un acceso básico ISDN, el cual tiene dos canales de 64 Kbps, lo cual hace una velocidad total de 128 Kbps tal y como se muestra en la figura (además se dispondría de un canal D de señalización el cual no tiene relevancia en este cuadro de diálogo). Dentro de los distintos tipos de conmutador, la opción más interesante es "*automation detection type*", con lo cual el programa lo detectará de manera automática, algo muy útil cuando se desconoce el tipo de conmutador. Para el caso concreto de este proyecto la interfaz

ISDN no va a ser utilizada, aunque no estaría de más su configuración para posteriores usos.

Una vez configurada la interfaz ISDN, se pulsa *"OK"* y aparece la siguiente caja de diálogo:

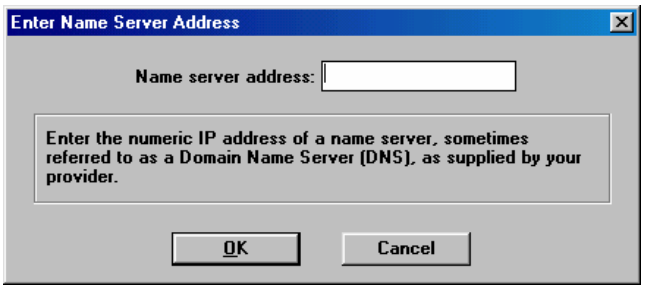

Figura -2.17- Cuadro de diálogo en el que se introduce la dirección del servidor de nombres

Aquí se especifica el nombre o la dirección IP del servidor de nombres (DNS). En nuestro caso se introducirá como servidor de nombre el servidor *ittest.upct.es* Una vez introducido el nombre y pulsado *"OK"* aparecerá la siguiente caja de diálogo:

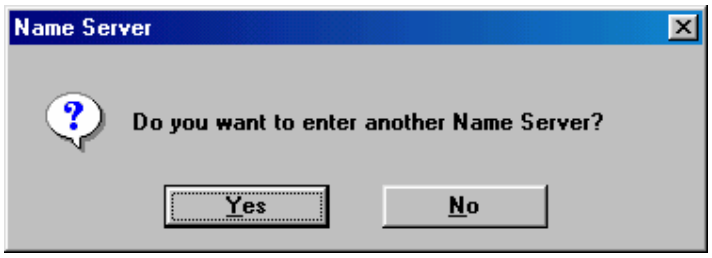

Figura -2.18- Cuadro de diálogo en el que se ofrece al usuario la opción de añadir otro servidor de nombres

La cual ofrece la opción de añadir algún otro servidor de nombres a la lista. Según las preferencias del usuario éste elegirá *Yes* o *No*. Hacemos click sobre la segunda opción.

Una vez terminada la lista de servidores DNS, ha finalizado la configuración inicial de la unidad, hecho que se comunica al usuario mediante el siguiente cuadro de diálogo:

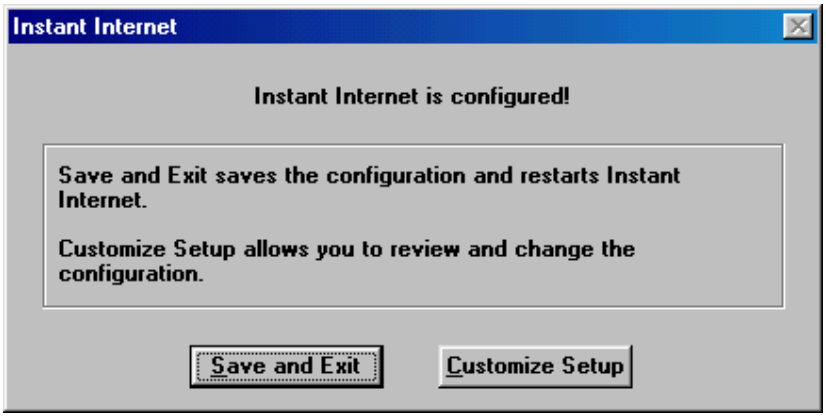

Figura -2.19- Cuadro de diálogo en el que se pueden guardar los cambios efectuados o proseguir la configuración

Desde aquí, pueden elegirse dos opciones:

- Salvar la configuración hecha hasta el momento y salir del programa. De este modo lo que el programa hará será reiniciar el conmutador para que los cambios realizados se actualicen.
- Continuar con una configuración específica para requisitos particulares, guardando todos los cambios más adelante desde la ventana *"Setup"*.

Elegimos la primera opción, para de este modo guardar la configuración inicial que se ha realizado de la unidad *Contivity 400*.

Configuración básica de *Contivity 400*

Una vez terminada la instalación del *software*, ya aparece en pantalla la ventana *"Setup"*, en la que, de momento, sólo puede apreciarse la interfaz *eth1*, además de la interfaz ISDN (la cual aparece configurada como ruta por defecto para salir al exterior), que es la que se configura por defecto con la dirección IP que se le ha otorgado a la unidad.

El siguiente paso es añadir el resto de interfaces del conmutador a la lista, para lo cual se hace uso del botón *Add* de la ventana *"Setup"*.

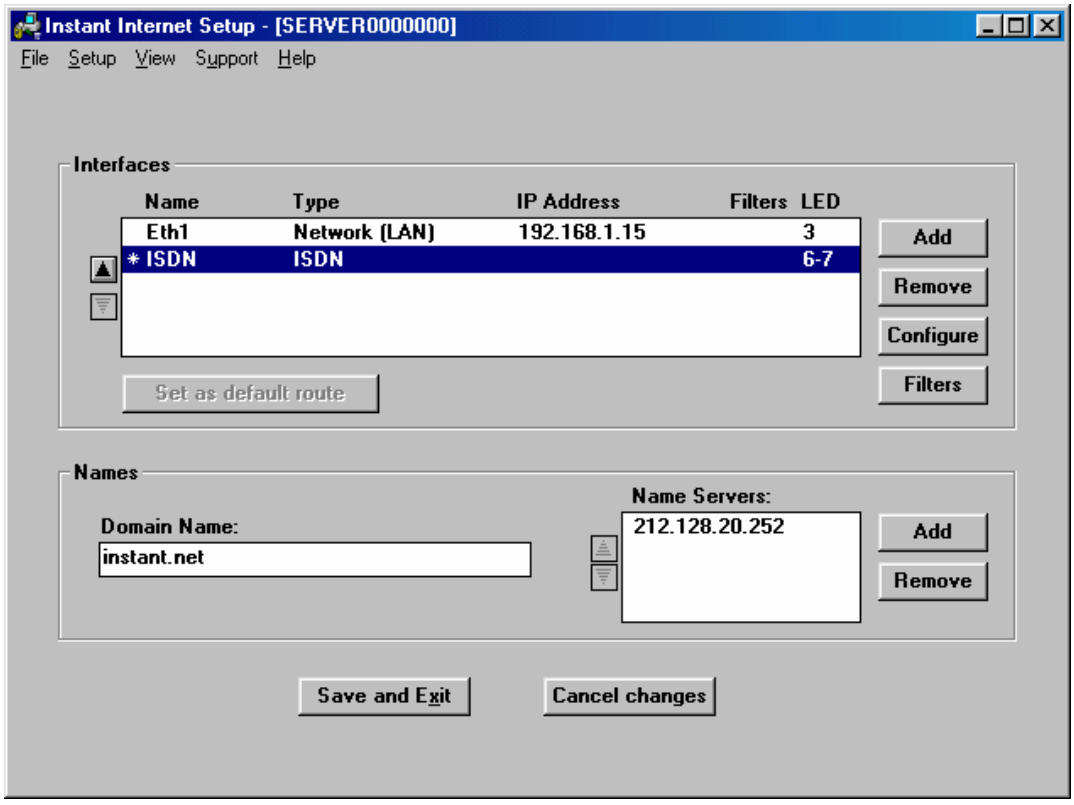

Figura -2.20- Ventana *"Setup"*

Para el desarrollo de este ejercicio se va a hacer uso de la arquitectura DMZ, cómo solo se dispone de una unidad *Contivity 400* será necesario configurar sus tres interfaces de red, con lo estaremos en el caso de una arquitectura DMZ con un único encaminador que posee tres o más interfaces de red. Para más información sobre este tipo específico de arquitectura y sobre la arquitectura DMZ en general léase el apartado 2.1.4.

Tras pulsar el botón *Add* se nos muestra un cuadro de diálogo en el que puede elegirse el tipo de interfaz que se desea añadir:

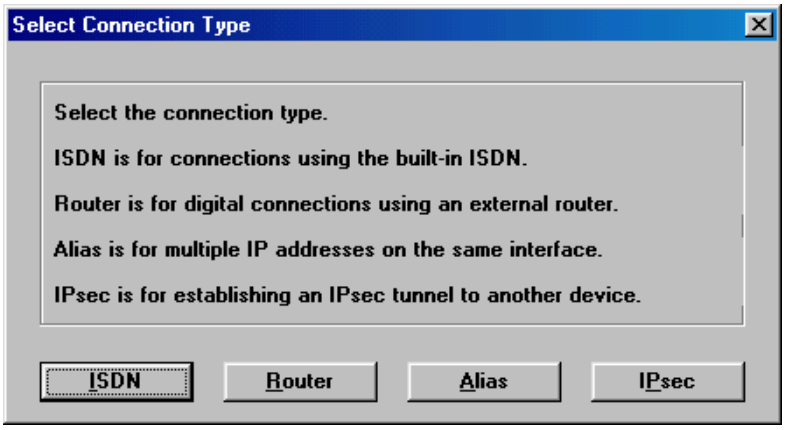

Figura -2.21- Cuadro de diálogo *Select Connection Type*

Como puede apreciarse en la figura, aparece la opción *Router*, esto es debido a que no hay seleccionada ninguna interfaz como ruta por defecto. En el momento que se configura alguna de las interfaces como ruta por defecto, cuando vaya a añadirse una nueva interfaz, en donde antes aparecía *Router* ahora aparecerá *Network*, refiriéndose a una interfaz para la conexión a redes de área local. En nuestro caso la interfaz ISDN ya aparece configurada como ruta por defecto, por lo que nos aparecerá una ventana de selección del tipo de interfaz con la opción *Network* en lugar de la opción *Router*. Pero al no hacer uso de dicha interfaz ISDN, vamos a definir como ruta por defecto una de la tres interfaces de red de las que dispone la unidad Contivity 400, concretamente la interfaz *eth2*. Por lo tanto, elegimos la opción *Router* y continuamos con la configuración.

Además de los tipos de interfaces mencionados anteriormente, puede elegirse también entre los tres siguientes tipos de interfaces:

- *ISDN*: Para interfaces que proporcionen el acceso a redes digitales de servicios integrados.
- *Alias*: Se hace uso de esta opción para poder asignar varias direcciones IP a un mismo dispositivo físico, una misma interfaz de red.
- *IPsec*: Es el Acrónimo de *Internet Protocol Security*. Que es un conjunto de protocolos que soportan IP y que introducen características de seguridad antes no contempladas, permite agregar encriptado y autenticación a las comunicaciones IP. *IPsec* se puede usar directamente entre las máquinas que se comunican, o bien a través de un túnel entre los dispositivos periféricos, llamados *gateways de seguridad*, que las conectan a través de Internet. Las formas de conectividad resultantes se llaman así *modo transporte* y *modo túnel* respectivamente.

Tras elegir el tipo de interfaz, aparece un cuadro de diálogo en el cual se escoge la interfaz que quiere configurarse:

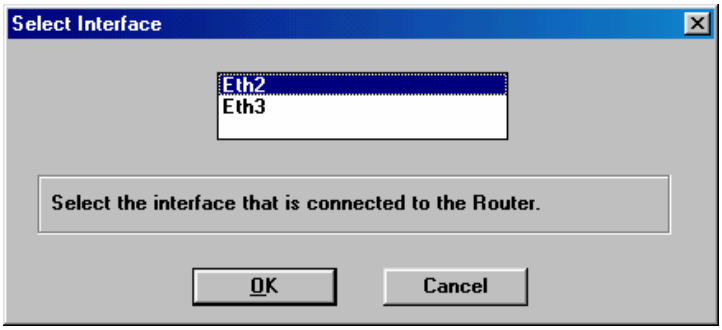

Figura -2.22- Cuadro de diálogo en el que se selecciona la interfaz a configurar

Se selecciona la interfaz que va a estar conectada al encaminador y la que va a actuar como ruta por defecto, es decir, la que va a proporcionar salida al exterior. Una vez seleccionada la interfaz aparece el cuadro de diálogo siguiente:

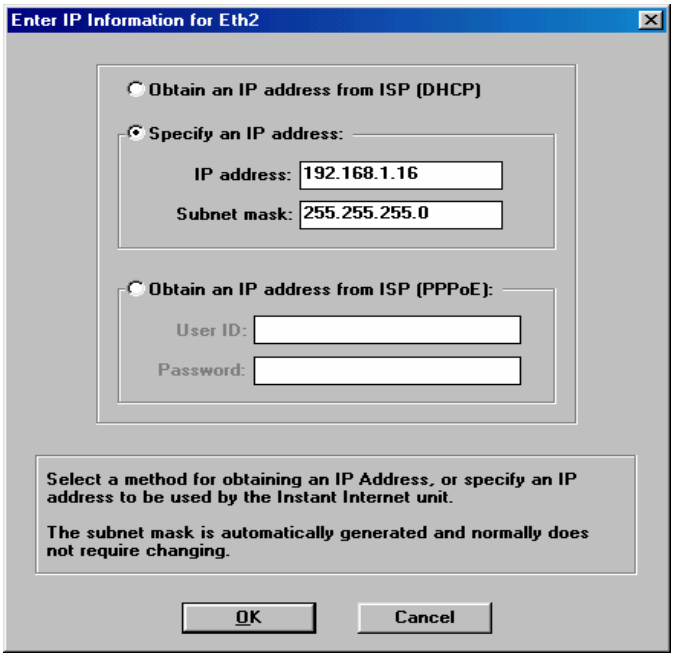

Figura -2.23- Cuadro de diálogo en el que se introduce la información correspondiente a una determinada interfaz que va a ser usada como ruta por defecto

En el cual se escoge la opción *Specify an IP adress*, asignándole a la interfaz en cuestión una dirección IP (la cual debe estar siempre dentro del rango perteneciente a red del equipo desde donde se está configurando el conmutador), una vez hecho esto, automáticamente el programa rellenará el campo *Subnet mask*, con las máscara de red apropiada para la dirección IP que se ha especificado. Se pulsa *"OK"* y aparece el siguiente cuadro de diálogo

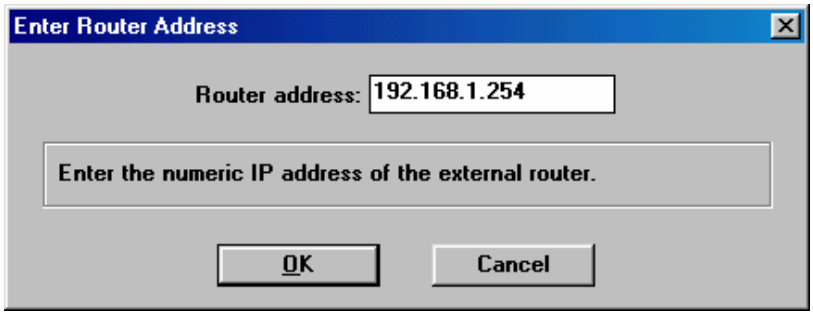

Figura -2.24- Cuadro de diálogo en el que se introduce la dirección del encaminador

Donde se especifica la dirección IP del encaminador de la red, el cual proporciona acceso al exterior, es decir, actúa como puerta de enlace o *gateway*. En nuestro caso concreto, la máquina que va a actuar como puerta de enlace va a tener la dirección IP *192.168.1.254*.

NOTA: En caso de que se trabajase con la interfaz ISDN como ruta por defecto para completar este ejemplo de configuración, simplemente se definirían las dos interfaces, *eth2* y *eth3*, como interfaces para la conexión a redes de *ethernet* tal y como se explica a continuación para la interfaz *eth3*.

Una vez que ya está definida una interfaz como ruta por defecto, se añade otra interfaz, en este caso particular la interfaz *eth3*, y puede observarse como ahora en el cuadro de diálogo de elección del tipo de interfaz, en lugar de aparecer como una de la opciones *Router* aparece la opción *Network*. Una vez elegida el tipo de interfaz que se quiere añadir aparece directamente el cuadro de diálogo para la configuración de la interfaz *eth3* ya que es la única que queda por añadir y configurar, se pulsa *"OK"* y aparece el cuadro de diálogo que se muestra en la figura 22:

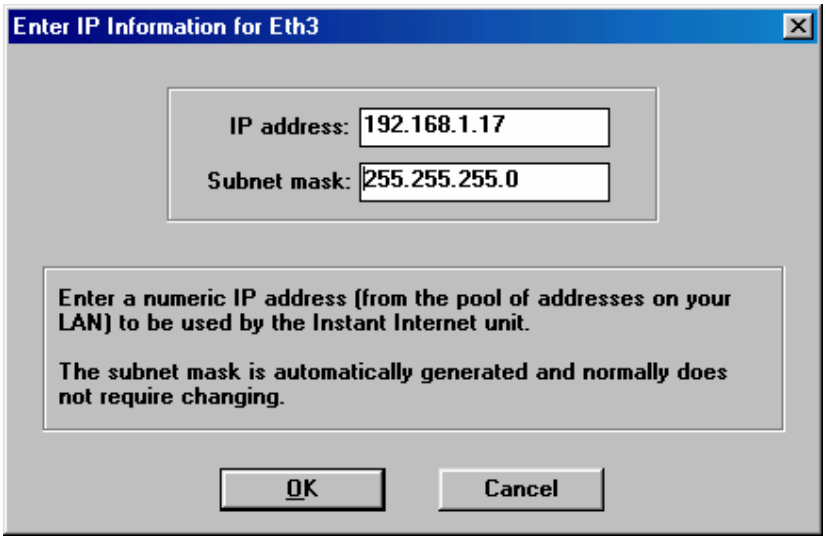

Figura -2.25- Cuadro de diálogo de información referente a una determinada interfaz

Se introduce la IP que se desee asignar a la interfaz y de nuevo el programa escribirá automáticamente la mascara de red. Se pulsa *"OK"* y queda añadida y configurada la interfaz en cuestión.

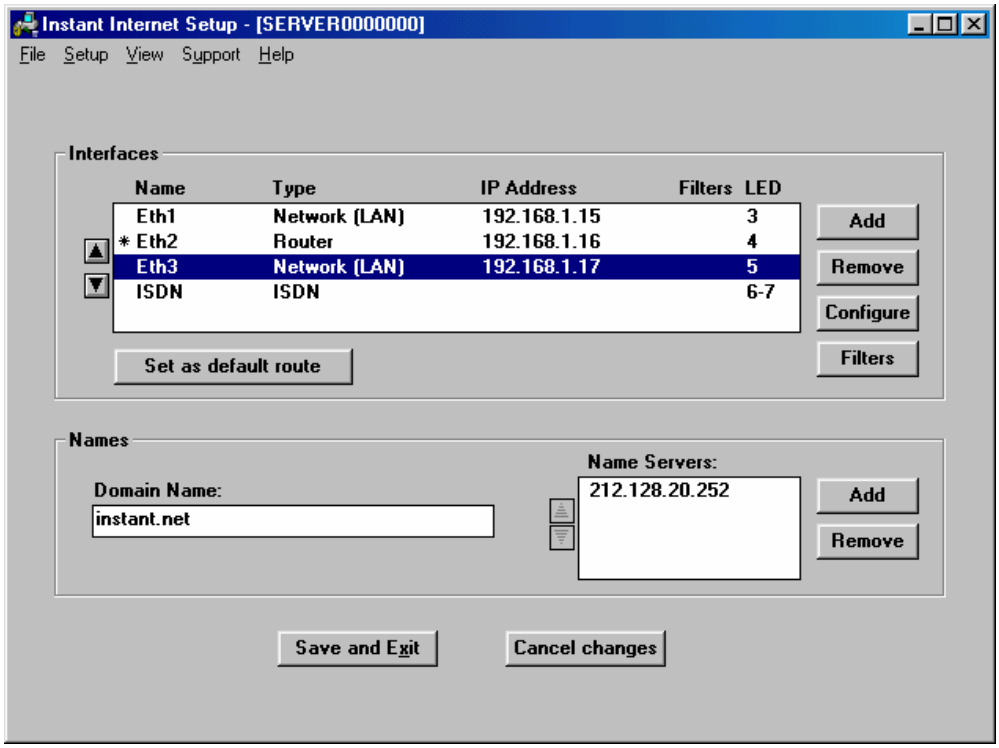

Figura -2.26- Ventana *"Setup"* una vez añadidas las interfaces de la unidad *Contivity 400*

A esta altura, en la ventana *"Setup"* se muestran las 3 interfaces de red de la unidad Contivity 400, cada una de ellas con sus correspondientes características.

Copia de los archivos de instalación

Desde la ventana *"Setup"* al guardar los cambios y salir de la misma mediante el botón *Save and Exit*, el programa de instalación ofrece la opción de elegir un directorio donde instalar el mismo:

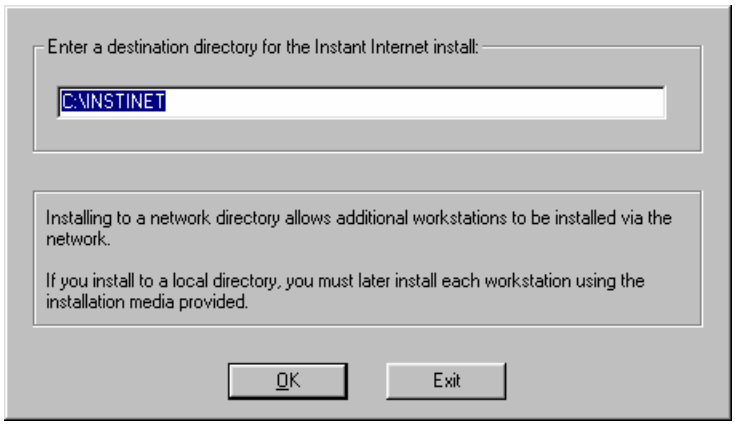

Figura -2.27- Cuadro de diálogo en el que se introduce el directorio en donde se instalará el *software*

Puede dejarse el que viene por defecto (recomendado) o indicar alguna otra ubicación. Se pulsa *"OK"* y a continuación se abre una caja de diálogo en la cual puede elegirse los componentes a instalar, en este caso solo hay un único componente el cual aparece marcado por defecto:

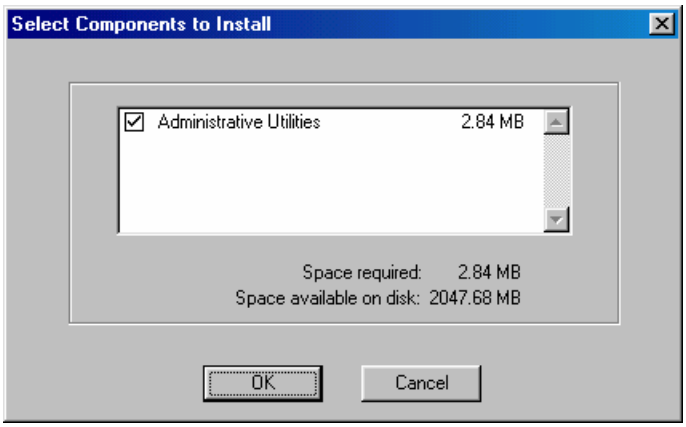

Figura -2.28- Cuadro de diálogo donde se eligen los elementos a instalar

Nos limitamos a pulsar *"OK"* el programa de instalación comienza la copia de archivos:

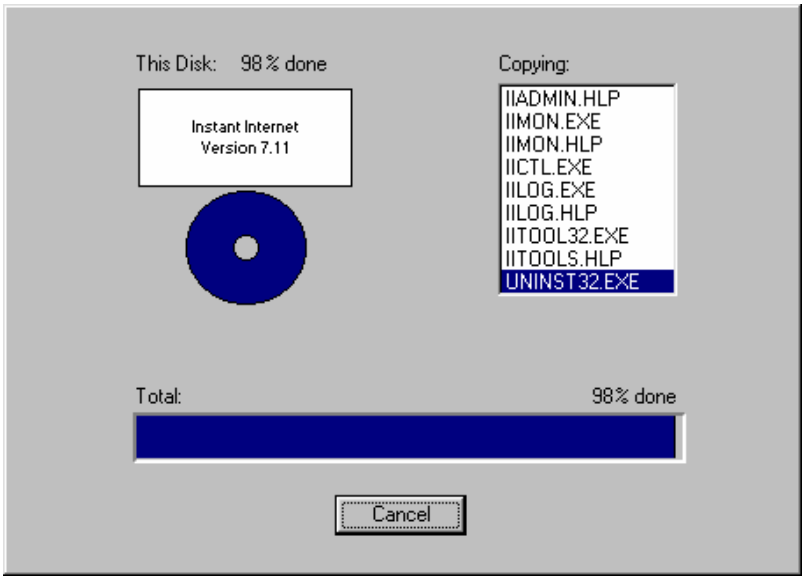

Figura -2.29- Ventana donde se muestra el proceso de la instalación

Indicando el programa la finalización de la misma mediante el siguiente cuadro de diálogo:

Figura -2.30- Cuadro de diálogo que informa del término de la instalación

Una vez que hemos llegado a este punto, es conveniente hacer algunas pruebas para verificar el correcto funcionamiento de lo configurado. Para ello se usar simplemente el comando "*ping*" que consiste en el envío de paquetes ICMP (Protocolo de Mensaje de Control de Internet) a una dirección especificada, la cual en caso de poder recibir dichos paquetes responde a la máquina que se los envió. Este comando es muy útil para comprobar lo que se denomina como "*visibilidad*" en una red, que se refiere a qué equipos pueden tener contacto entre sí, es decir, que equipos "se ven".

Por tanto, se hace ping a diferentes puntos de la red, siendo puntos clave de esta comprobación, el encaminador y el servidor DNS. Un vez llevadas a cabo con éxito estas pruebas ya se tiene configurada lo que se definiría como "parte *hardware*" del conmutador.

NOTA: Todo lo mencionado anteriormente en cuanto a configuración de la interfaces consiste en un ejemplo en el que se configuran todas la interfaces para la conexión a una red local, siendo una de ellas definida como ruta por defecto. Esto no quiere decir que no sea factible cualquier otro tipo de configuración de las interfaces tales como ISDN, Alias o IPsec, según las necesidades del usuario.

2.2.3.2 Configuración específica de Contivity 400 para cumplir los requisitos del ejercicio propuesto

El primer paso es encender la unidad *Contivity 400*, y cuando el LED 2 esté de con luz verde fija, nos vamos al *software* **Instant Internet** que acompaña al *Contivity* para su gestión y se pulsa la opción *"Setup"* para entrar en la ventana de gestión de la unidad.

NOTA: Se supondrá realizada la instalación del *software* y la asignación de una dirección IP a la unidad *Contivity 400* tal y como se describió en el apartado 2.3.3.1.

En dicha interfaz puede observarse que ya hay una interfaz, en concreto la *eth1,* con una dirección IP asignada (que es la dirección IP asignada a la unidad *Contivity* en la configuración inicial vista en el capitulo anterior). Ahora hay que añadir las dos interfaces restantes, para ello se pulsa el botón *Add* del cuadro *"Setup"* y aparecerá un cuadro como el de la figura 30, en el que se pulsa la opción *Network*, para añadir una

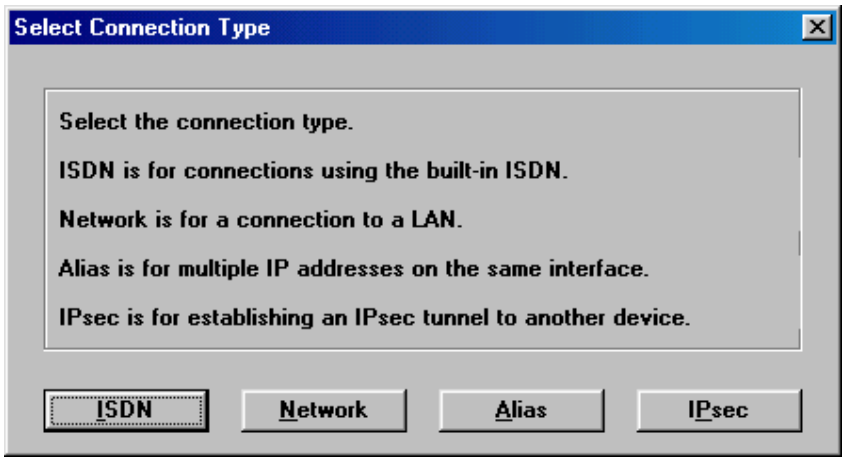

FIGURA-2.31 - Cuadro de selección del tipo de interfaz

interfaz de red para la conexión a redes locales, una vez elegido el tipo de interfaz aparecerá un cuadro como el de la figura 31 en el que elegir que interfaz

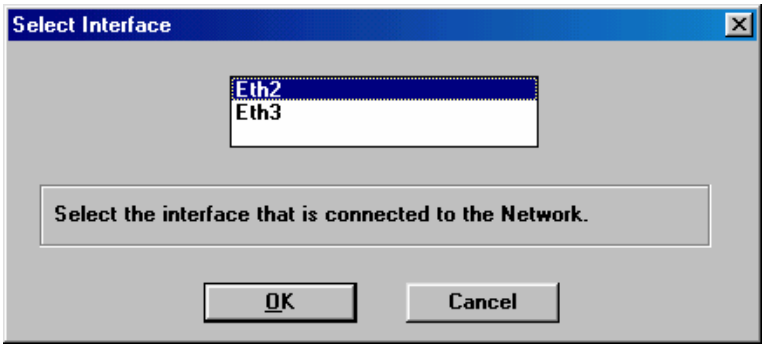

FIGURA -2.32 - Cuadro de selección de interfaz

se quiere usar. Se elige la interfaz *eth2* y se pulsa *"OK"* en el cuadro de selección de interfaz y aparece un cuadro como el de la figura 32 en el que se introducen los datos pertenecientes a la interfaz, tales como su dirección IP y la máscara de red. Se introduce la dirección *192.168.2.1* dejando en blanco el campo de la máscara de red, lo que equivale a escribir el valor *255.255.255.255*.

Siguiendo el mismo proceso se añade la interfaz *eth3* pero esta vez asignándole la dirección IP *192.168.3.1*.

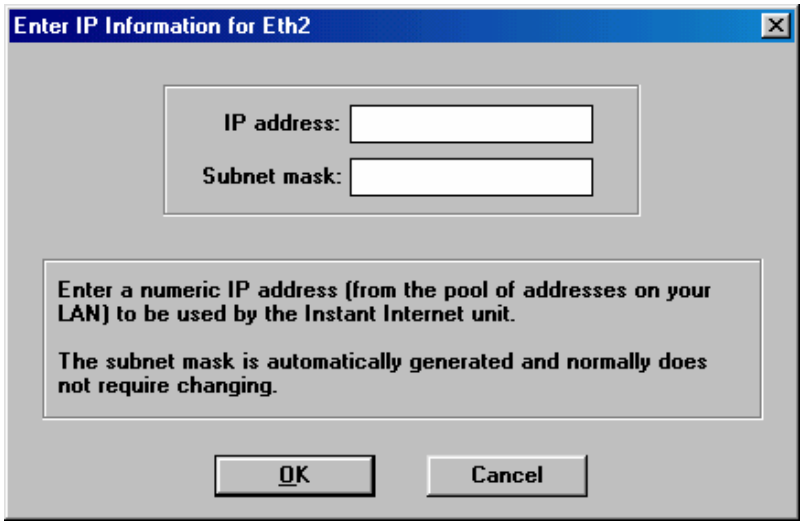

FIGURA -2.33- Cuadro de información sobre la interfaz

Una vez añadidas las 3 interfaces de red del *Contivity 400* comienza la configuración de las mismas para los requisitos planteados:

INTERFAZ 1 (Red Externa):

En esta interfaz, al ser la que se corresponde con la Red Externa, se permite la entrada sólo a los paquetes que tengan como dirección destino el *proxy*, mientras que se restringe la salida a cualquier paquete excepto a aquellos provenientes del Servidor *Proxy* que es el que proporciona el acceso al exterior (y por lo tanto a Internet) de todos los PC de la Red Interna.

Filtros de Entrada:

Se usa un filtro de entrada que sólo permita el paso a los paquetes cuya dirección destino sea la 192.168.3.1 (Servidor *Proxy*). Para ello se selecciona la interfaz *eth1* y se pulsa el botón *Filters* en la ventana *"Setup"* (mostrada en la figura 33), accediendo de este modo al

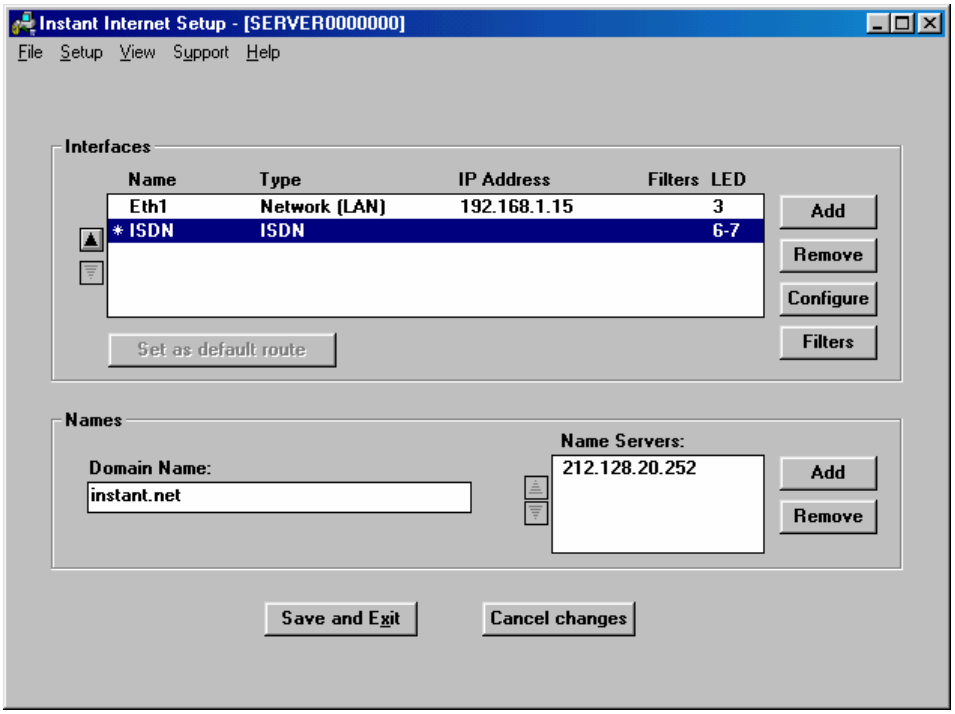

FIGURA -2.34- Ventana *""Setup""* del *software* de gestión del contivity.

Cuadro de configuración de filtros para la interfaz *eth1*, en donde se pulsa el botón *Add* para añadir un nuevo filtro a la lista de filtros. Una vez situados en el cuadro de diálogo de configuración del filtro se le van añadiendo reglas mediante el botón *Add*.

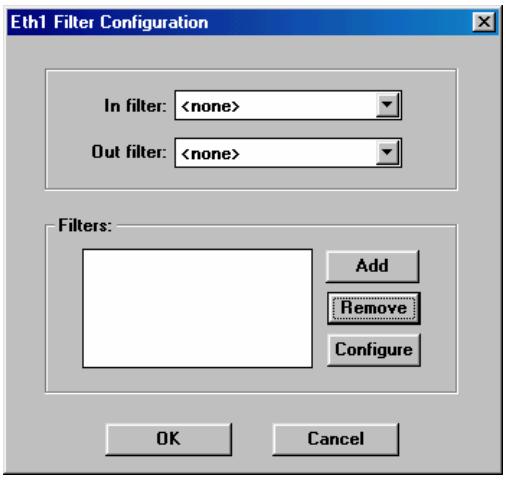

FIGURA -2.35 - Cuadro de configuración de filtros de la interfaz *eth1*

En este caso se añade una única regla que permite el paso a todo los paquetes cuya dirección destino sea la 192.168.3.1, para ello en el cuadro de diálogo de creación de reglas, se marca la opción **Action** como *Allow*, en **Protocol** se escoge la

opción *TCP*, el campo **Source** se deja en blanco de modo que se permita cualquier dirección IP origen, en el campo **Destination** se especifica como dirección destino en **Address** la 192.168.3.1 y el rango de puertos se deja en blanco de modo que se permita el acceso a todos los puertos de dicha máquina destino. No es necesario especificar el número de bits de la porción de red (dejando el que hay por defecto, es decir, 32).

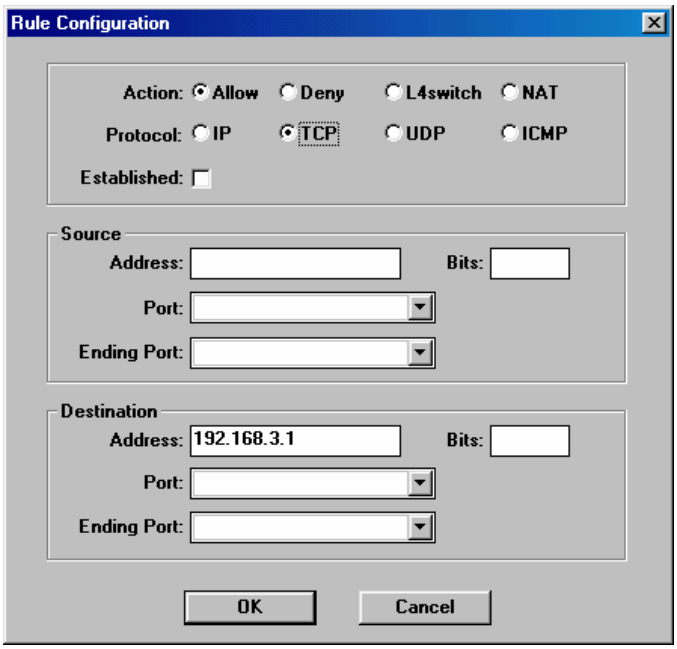

FIGURA -2.36 - Cuadro de configuración de reglas

Filtros de salida:

- Los paquetes son filtrados mediante un filtro de salida que sólo deje salir al exterior aquellos paquetes que provengan del servidor *Proxy* (es decir, cuya dirección fuente sea la del servidor *Proxy*).
- Se permitirán sólo tres puertos: el puerto 80 (HTTP), el 443 (SHTTP) y el 22 (SSH).

Para cumplir estas condiciones se necesita configurar un filtro de salida, para ello en el cuadro de la figura 33 se selecciona la interfaz *eth1* y se pulsa el botón *Filters* apareciendo un cuadro de configuración de filtros para la interfaz *eth1* como el que se muestra en la figura 34. Dentro de dicho cuadro se pulsa el botón *Add* de forma que aparece un cuadro para crear un nuevo filtro como el que se muestra en la figura 36.

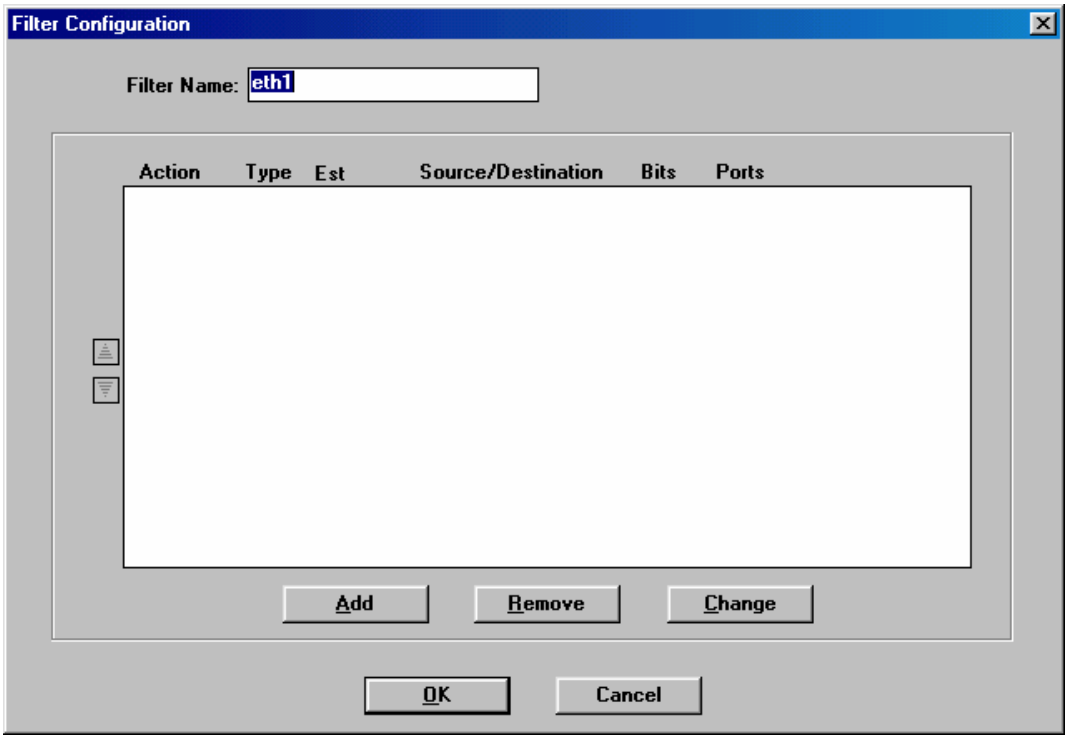

FIGURA -2.37- Cuadro de diálogo de configuración del filtro

En este cuadro de diálogo en la caja de texto *Filter Name*, se especifica el nombre del filtro, que en este caso será *F.Salidaeth1*. Una vez especificado el nombre del filtro se pasa a añadir las reglas que lo componen, para ello se pulsa el botón *Add*, y aparece un cuadro de diálogo como el que se puede observar en la figura 35, donde se puede definir una regla que formará parte del filtro. En nuestro caso, la primera regla que se define es aquella que sólo deja salir al exterior los paquetes con dirección origen la del servidor *Proxy*, para ello en la figura 35 en **Action** se marca la opción *Allow*, en **Protocol** se activa la casilla correspondiente a *TCP*, dentro de **Source** en **Address** se escribe la dirección del servidor *Proxy* que en nuestro caso es la *192.168.3.1*, no es necesario especificar el número de bits de la porción de red (dejando el que hay por defecto, es decir, 32), en cuanto a los puertos sólo se permitirán tres, tanto origen como destino, el puerto 80 (HTTP), el 443 (SHTTP) y el 22 (SSH), por lo tanto habrá que crear tres reglas, todas ellas idénticas exceptuando el campo **Port** de la opción **Source** en el que se introduce en cada una el número del puerto correspondiente. En cuanto **Destination** se deja en blanco, es decir, se permite cualquier dirección y puerto destino. Para el caso del puerto 80 el cuadro de configuración de reglas quedaría tal y como se muestra en la figura 37. Se pulsa el botón *"OK"* y la regla queda configurada y añadida a la lista de reglas del filtro. El resto de reglas se crearían del mismo modo pero fijando el valor del campo **Port**

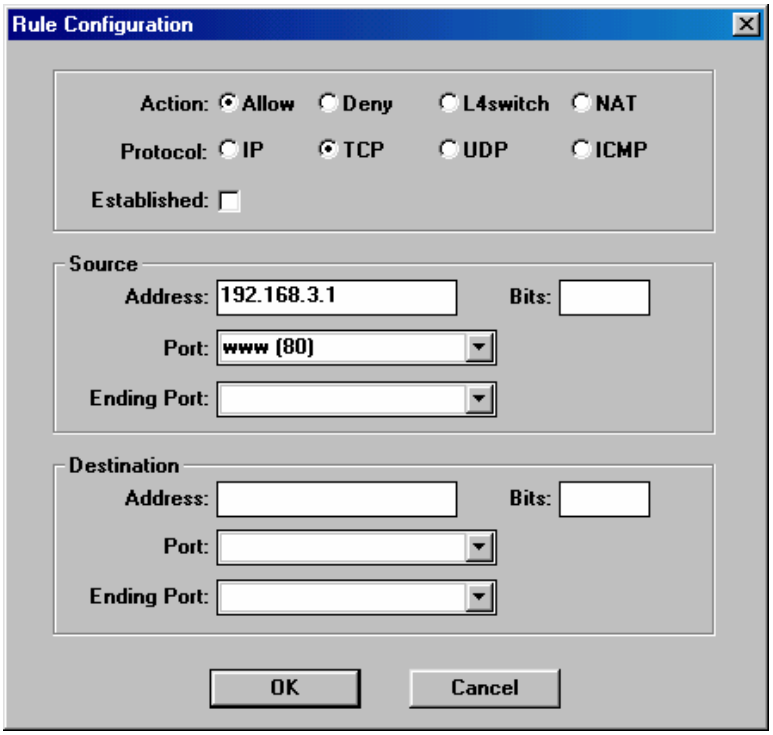

FIGURA -2.38- Cuadro de configuración de reglas

correspondiente. Recordemos que si no se cumple ninguna de las reglas de la lista del filtro el *Contivity 400* por defecto deniega el paquete, aún así se puede añadir al final de la lista una regla que deniegue todos los paquetes.

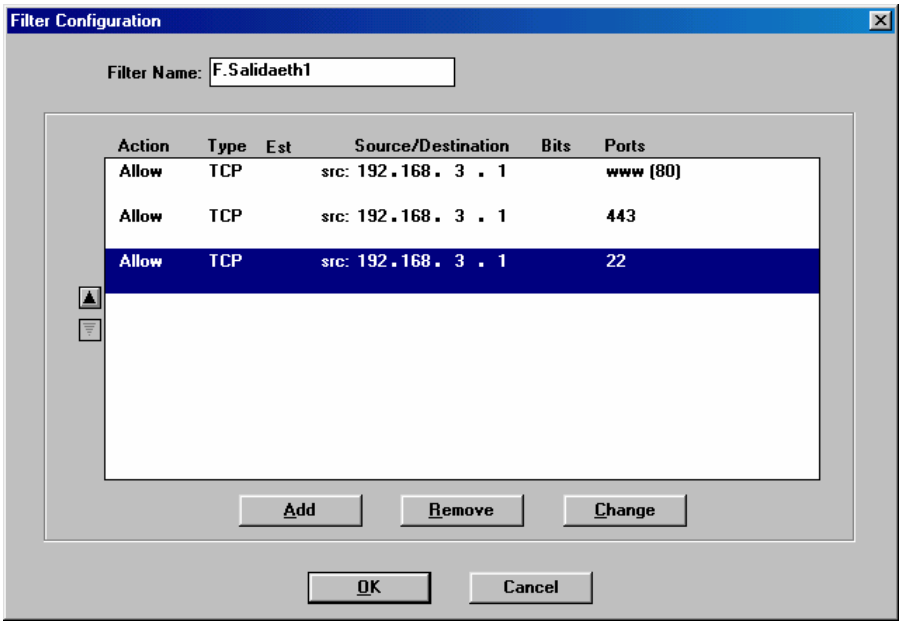

FIGURA -2.39- Cuadro de configuración del filtro

Una vez añadidas todas las reglas en la ventana de configuración del filtro, para finalizar, se pulsa *"OK"* volviendo al cuadro de diálogo de configuración.

Una vez configurados los filtros de entrada y de salida para la interfaz *eth1*, desde la ventana de configuración de filtros para la interfaz *eth1* en el menú desplegable *In filter* se escoge el filtro *F.Entradaeth1* y en el menú desplegable *Out filter* se escoge *F.Salidaeth1* como filtro de salida para la interfaz *eth1*, quedando el cuadro de configuración de filtros tal y como se muestra en la figura 39:

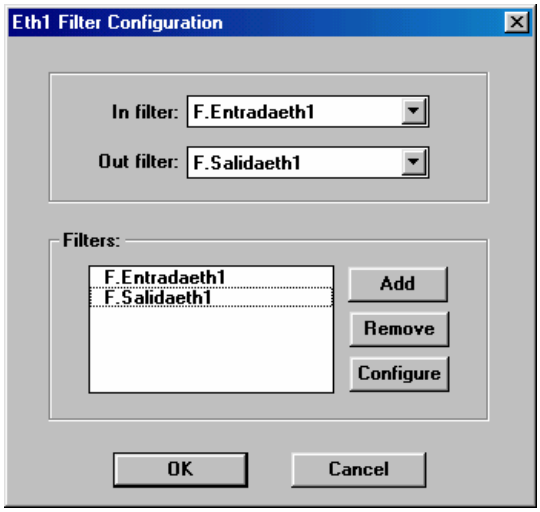

FIGURA -2.40- Filtro *F.Salidaeth1* aplicado como filtro de salida de la interfaz eht1

Una vez hecho esto, en el cuadro de configuración de filtros para la interfaz *eth1* se pulsa *"OK"* y ya está configurada la interfaz *eth1* con los filtros necesarios para cumplir los requisitos de la práctica planteada.

Para comprobar si se va a aplicar algún filtro a una interfaz basta con mirar en la ventana *"Setup"* si aparece marcada la columna *Filters* en la fila correspondiente a la interfaz en cuestión. En nuestro caso para la interfaz 1, una vez que ya está aplicado el filtro *F.Salidaeth1* la ventana *"Setup"* presentará aspecto que se muestra en la figura 40:

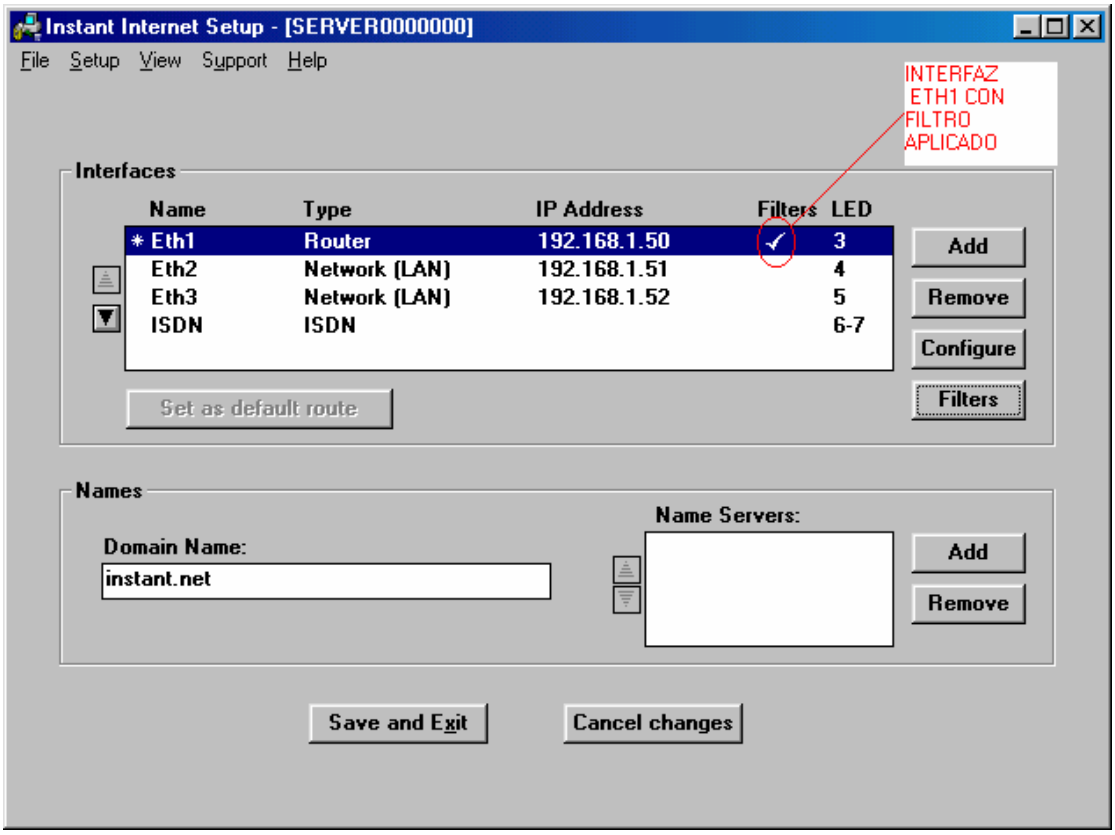

FIGURA -2.41- Ventana *"Setup"*

Se puede apreciar como la fila correspondiente a la interfaz *eth1* aparece marcada en la columna *Filters* indicando que hay algún filtro aplicado a la interfaz *eth1*.

INTERFAZ 2 (Zona DMZ)

En la interfaz *eth2* se permite a la entrada cualquier paquete dirigido al servidor de Correo a través de los puertos 220, 110 y 25 (IMAP3, POP3 y SMTP respectivamente) o dirigido al Servidor Web a través de los puertos 80 y 443 (HTTP y HTTPS respectivamente). En cuanto a la salida, por la interfaz *eth2* sale cualquier tipo de paquete con cualquier dirección y puerto fuente o destino.

Filtro de Entrada :

- Se permite pasar los paquetes con cualquier dirección fuente y dirección destino el servidor de correo y puertos destino POP3, IMAP3 y SMTP,
- Son permitidos también los paquetes con dirección destino el servidor Web y a través de los puertos HTTP y HTTPS.

Para configurar un filtro de estas características, dentro de la ventana *"Setup"*, se selecciona la interfaz *eth2* y pulsando el botón *Filters*, se pasa al cuadro de diálogo de configuración de filtros (figura 34), pero en este caso para la interfaz *eth2*, una vez aquí se pulsa el botón *Add* pasando al cuadro de creación de filtros (figura 36), donde se le asigna al filtro el nombre de *F.Entradaeth2*. Una vez asignado el nombre dentro de la ventana de configuración del filtro se pulsa el botón *Add* para añadir la primera

de las reglas del filtro mediante el cuadro que se muestra en la figura 35. En primer lugar se añade la regla que permita la entrada de paquetes con dirección destino el servidor de correo y puerto destino el POP3, para ello basta con marcar *NAT*, de forma que se permita el uso de la traducción de direcciones con los paquetes en cuestión, en la zona **Action**, dentro de **Protocol** se se marca *TCP*, **Source** se deja en blanco, de modo que se permita la entrada de paquetes con cualquier dirección origen y desde cualquier puerto. En **Destination** se especifica como dirección destino la *192.168.2.2* y puerto destino el 110(POP3). Tras realizar todas las operaciones citadas anteriormente, el cuadro de configuración de reglas quedará tal y como se muestra en la figura 41.

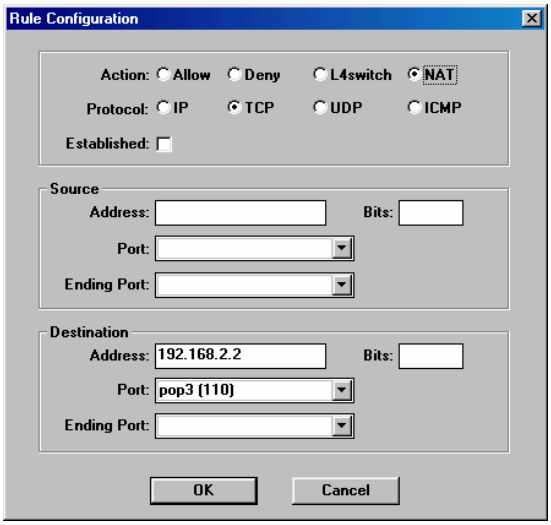

FIGURA -2.42- Cuadro de configuración de reglas particularizado para unos requisitos determinados

Dentro del cuadro de configuración de reglas se pulsa *"OK"* y la regla es añadida la lista de reglas del filtro.

La siguiente regla que añadimos es similar a ésta, pero con la diferencia que el puerto que destino que se permite será el SMTP. Para ello se repiten todos los paso citados anteriormente excepto a la hora de fijar el puerto destino, que se pone como tal el 25 que es puerto que se corresponde con SMTP. El cuadro de configuración de reglas queda por tanto tal y como se muestra en la figura 42:

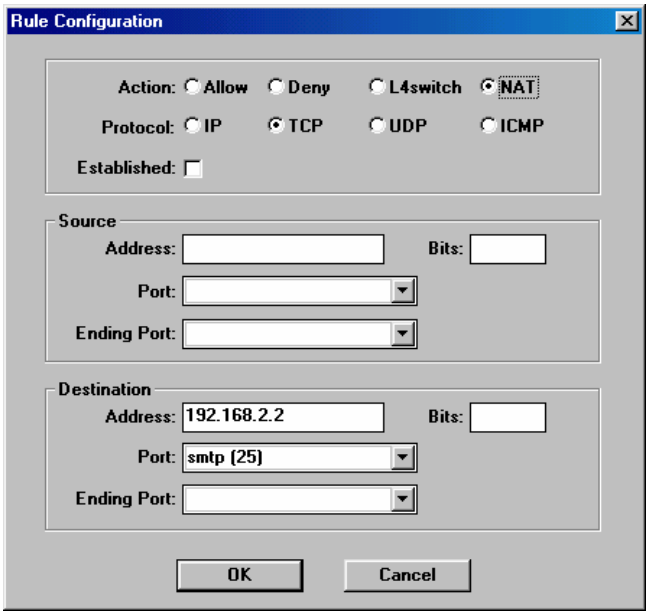

FIGURA -2.43- Cuadro de configuración de reglas particularizado para unos determinados requisitos

Dentro del cuadro de configuración de reglas se pulsa *"OK"* y la regla es añadida la lista de reglas del filtro.

A continuación se repite la misma operación pero esta vez para permitir IMAP3, siguiendo el mismo proceso que en los dos casos anteriores pero fijando esta vez como puerto destino el 220. La ventana de configuración de esta regla se muestra en la figura 43.

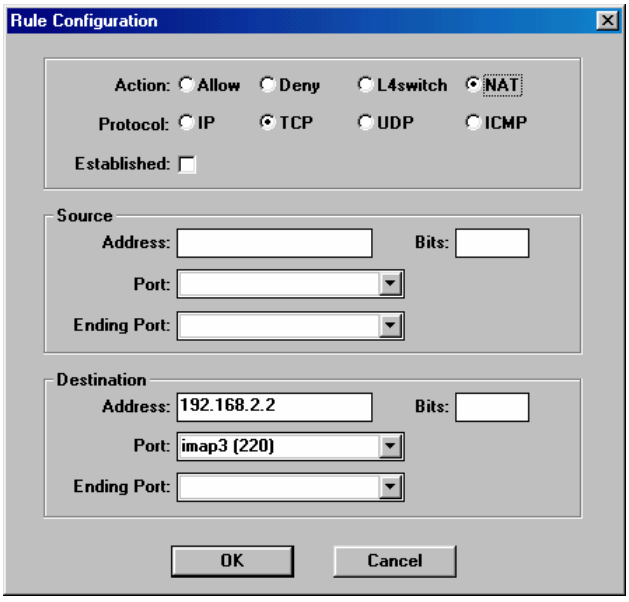

FIGURA -2.44- Cuadro de configuración de reglas particularizado

Dentro del cuadro de configuración de reglas se pulsa *"OK"* y la regla es añadida la lista de reglas del filtro.

Ahora se configuran las reglas que afectan al servidor Web, en primer lugar se configura una regla que permita el acceso a dicho servidor a cualquier máquina a través del puerto 80 (HTTP) mediante NAT, para ello en el cuadro de definición de reglas (Figura 4) en **Action** se marca la opción *NAT*, en **Protocol** se marca como protocolo de los paquetes que ser verán afectados por esta regla el protocolo *TCP*. Los campos pertenecientes a **Source** se dejan en blanco para permitir cualquier dirección y puerto fuente, mientras que en **Destination** se marca como dirección destino la 192.168.2.1 (Servidor Web) y como puerto el 80 (HTTP). La figura 44 muestra el aspecto del cuadro de configuración de reglas una vez rellenados los campos con los valores específicos para esta regla.

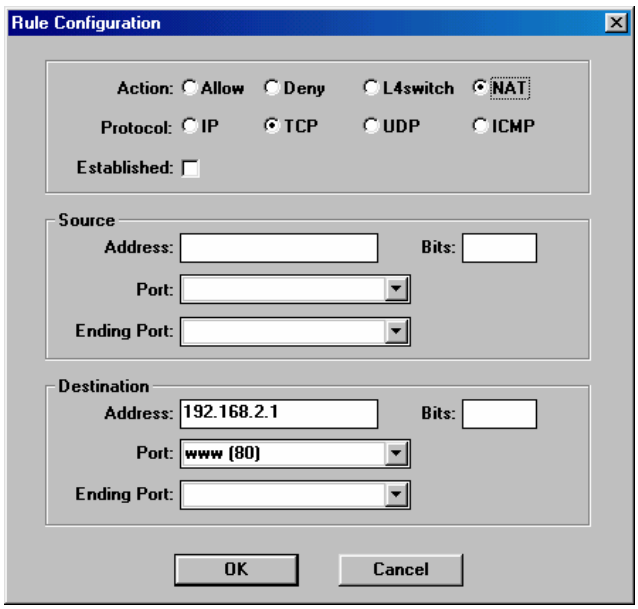

FIGURA -2.45- Cuadro de configuración de reglas particularizado

Dentro del cuadro de configuración de reglas se pulsa *"OK"* y la regla es añadida la lista de reglas del filtro.

Se añade ahora una regla similar a la anterior, pero esta vez que permita el puerto 443 (HTTPs), para ello solo se debe seguir el procedimiento llevado a cabo con la anterior regla y dentro de **Destination** fijar como puerto destino en **Port** el 443, quedando el cuadro de configuración de reglas de la siguiente forma:

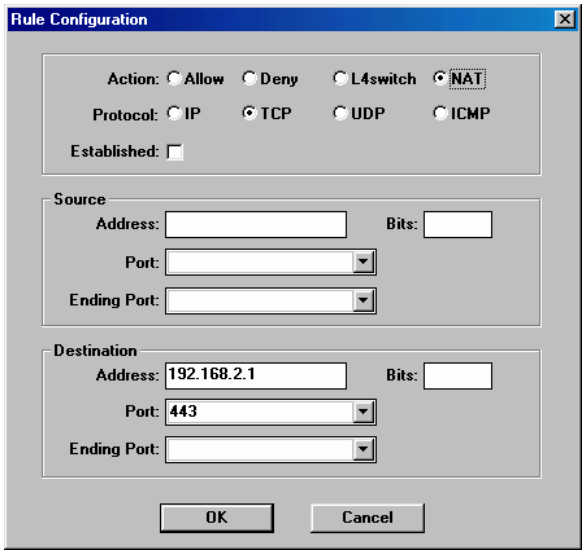

FIGURA -2.46- Cuadro de configuración de reglas particularizado

Dentro del cuadro de configuración de reglas se pulsa *"OK"* y la regla es añadida la lista de reglas del filtro.

Una vez añadidas todas la reglas citadas anteriormente a la lista de reglas del filtro, podríamos añadir una última regla que deniegue todos los paquetes para de este modo asegurarnos que no atraviese la interfaz ningún paquete no permitido, aunque no es estrictamente necesario, ya que la unidad *Contivity 400* deniega todos aquellos paquetes que atraviesen una interfaz a la cual se le aplica un filtro y no cumplan ninguna de las condiciones de las reglas de dicho filtro.

El cuadro de configuración del filtro de entrada *F.Entradaeth2* presentará entonces el aspecto que se muestra en la figura 46.

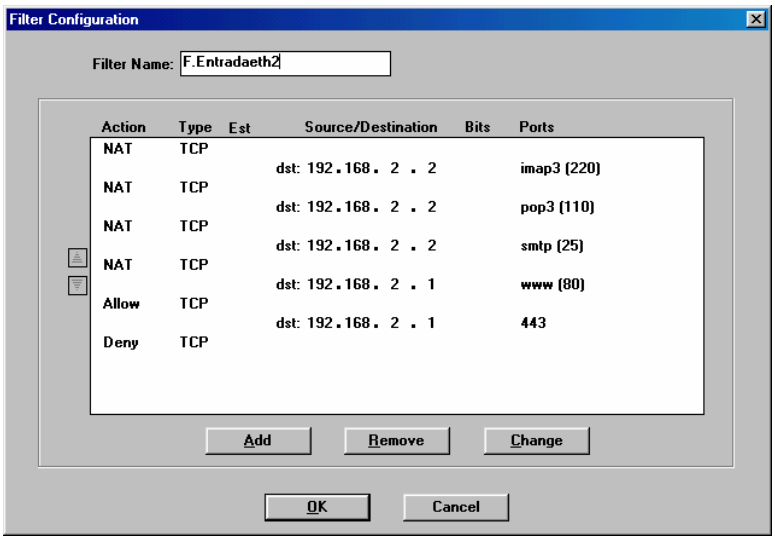

FIGURA -2.47- Cuadro de configuración del filtro F.Entrada*eth2*

Se comprueba que las reglas que componen el filtro son las que se necesitan y dentro de la ventana de configuración del filtro se pulsa *"OK"*. De este modo el filtro aparece ya en la lista de filtros seleccionables y por lo tanto aplicables a la interfaz que hay en el cuadro que muestra la figura 4 (lista en la cual ya estarán los filtros que hayan sido definidos con anterioridad para aplicarlos a la interfaz 1), en el cual en **In Filter** se selecciona del menú desplegable el filtro *F.Entradaeth2* y se pulsa *"OK"* en la ventana de configuración de filtros para la interfaz *eth2*.

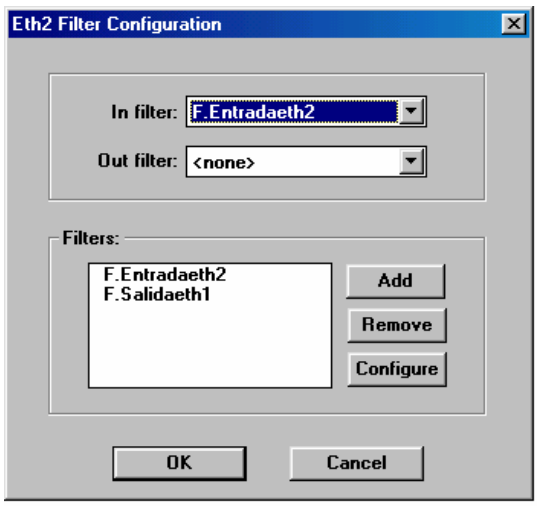

FIGURA -2.48- Cuadro de aplicación de filtros de interfaz *eth2*

Ya está configurada la interfaz *eth2* con el filtro de entrada F.Entrada*eth2* el cual cumple los requisitos especificados por el ejercicio.

Filtro de Salida:

No se usa ningún filtro de salida, dejando la situación por defecto, es decir, todos los paquetes permitidos. Por lo tanto bastará con verificar que en el cuadro de la figura 47 en **Out Filter** está seleccionado *<none>*, lo que indicará que no hay configurado ningún filtro como filtro de salida de la interfaz *eth2*.

Se pulsa *"OK"* en la ventana de configuración de filtros para la interfaz *eth2* y ya está configurada la interfaz *eth2* con los filtros adecuados para poder cumplir los requisitos especificados por la práctica.

INTERFAZ 3 (Red Interna)

En esta interfaz deben darse una serie de condiciones tales como que sólo puedan atravesarla paquetes provenientes del servidor Web con destino las bases de datos y el puerto 1521(puerto por defecto de la base de datos *Oracle*) o paquetes con dirección destino el servidor *Proxy*, ya que dichos paquetes se corresponderán con las respuestas de los sitios Web o máquinas de otras redes externas a las máquinas de la Red Interna que salen todas a través del Servidor *Proxy*. Pero sólo se deja, por cuestiones de seguridad, acceder a determinados puertos del Servidor *Proxy*, como son el HTTP, HTTPS Y SSH. Y en cuanto a los paquetes salientes, sólo pueden salir por esta interfaz las peticiones que hace el Servidor *Proxy* para comunicar a los PC de

la Red Interna con los PC de la Red externa, es decir, sólo pueden salir los paquetes con dirección origen la dirección del Servidor *Proxy*.

Filtro de Entrada :

Sólo se dejan entrar los paquetes provenientes del servidor Web con destino la Base de Datos y sólo a través del puerto 1521. Además se permite también la entrada de paquetes con dirección destino la del Servidor *Proxy*.

Para ello se selecciona la interfaz *eth3* en el cuadro *"Setup"* (Figura1) y pinchando sobre el botón *Filters*, se accede al cuadro de configuración de filtros de la interfaz *eth3* (Figura 47, pero para *eth3*) se pincha sobre el botón *Add* para crear un nuevo filtro. El filtro recibe el nombre de *F.Entradaeth3* escribiendo dicho nombre en el campo **Filter Name**. Una vez dotado de nombre el filtro es tiempo de crear y añadir las reglas que componen dicho filtro. Para ello dentro del menú de configuración del filtro (figura 36) se pulsa el botón *Add* entrando de este modo en el cuadro de creación de reglas (figura 35), en el cual en este caso como **Activity** se marca *Allows* y en **Protocol** se escoge la opción *TCP*. Dentro de **Source** se escribe como dirección fuente la 192.168.2.1 y cualquier puerto origen. En **Destination** como dirección destino se marca la 192.168.3.2 y fijando como puerto destino el 1521.

Una vez configurada la regla, dentro del cuadro de configuración de reglas se pulsa *"OK"* y la regla es añadida al filtro.

Se añade ahora la siguiente regla que consiste el permitir la entrada de paquetes con dirección destino y puerto 80 (HTTP). Para ello dentro del cuadro de definición de reglas para el filtro F.Entrada*eth3* se pulsa el botón *Add* accediendo de este modo al cuadro de configuración de reglas. En dicho cuadro se marca como **Action** la opción *Allow* fijando como *TCP* el campo **Protocol**. **Source** queda en blanco, permitiendo de este modo cualquier dirección o puerto origen y en **Destination** se especifica la dirección del Servidor *Proxy*, marcando también como el puerto destino el 80. Siguiendo este mismo proceso se añaden dos reglas más, una para permitir el puerto 443 (HTTPs) y otra para añadir el puerto 22 (SSH).

Una vez definidas todas las reglas, en el cuadro de configuración del filtro se pulsa *"OK"* y ya está creado el filtro y añadido a la lista de filtros aplicables a las interfaces. Ahora dicho filtro se le aplica a la interfaz desde el cuadro de configuración de filtros de la interfaz *eth3*, seleccionándolo como filtro de entrada en el menú desplegable de **In Filter**.

Filtro de salida:

- La Base de Datos podrás salir sólo hacia la zona DMZ y concretamente hacia el servidor Web y a través del puerto 1521.
- Permitiremos salir al servidor *Proxy* hacia cualquier zona.

Para cumplir estos requisitos se crea un filtro compuesto por dos reglas para ello en el cuadro de configuración de filtros de la interfaz (figura 34, pero particularizado para la interfaz *eth3*) se pulsa el botón *Add* entrando de este modo en el menú de configuración del filtro (figura 3) al que se le da el nombre de *F.Salidaeth3* escribiendo dicho nombre en el campo **Filter Name**, tras ésto se pulsa el botón *Add* para añadir una regla a la lista de reglas de nuestro filtro, una vez en el cuadro de definición de reglas (figura 4) se marca como **Action** la opción *Allows* y en **Protocol** se escoge *TCP*. En cuanto a **Source** se especifica como dirección fuente la *192.168.3.2* dejando en blanco el puerto fuente, lo que indica que es válido cualquier puerto. En **Destination** se escribe como dirección destino la *192.168.2.1* y se fija como puerto

destino el 1521, quedando el cuadro de definición de reglas tal y como se muestra en la figura 48.

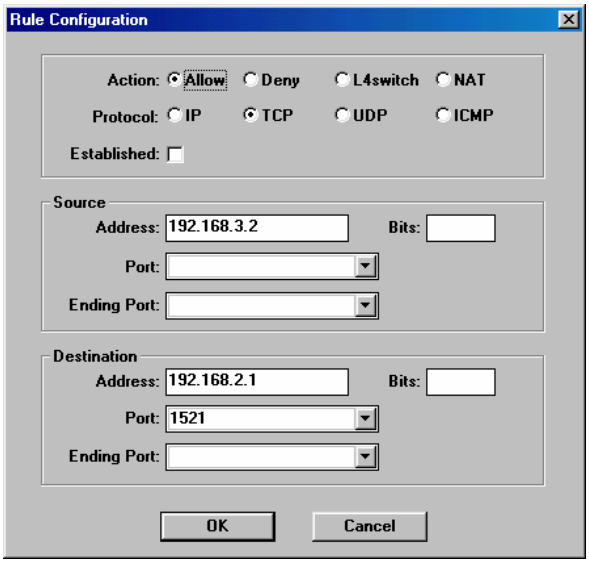

FIGURA -2.49- Cuadro de configuración de reglas particularizado

Falta definir una regla que permitiese la salida del servidor *proxy* al exterior, para ello dentro del cuadro de configuración del filtro se pulsa de nuevo el botón *Add* para añadir una nueva regla en la que se especifica como **Action** la opción *Allows*, marcando *TCP* dentro de **Protocol**. Dentro de **Source** se escribe como dirección fuente la *192.168.3.1* (Servidor *Proxy*) dejando en blanco la opción **Port**, permitiendo de este modo cualquier puerto origen. En **Destination** no se especifica dato alguno, permitiendo así cualquier dirección y puerto destino. Por tanto, el cuadro de definición de la regla quedaría configurado de la siguiente forma:

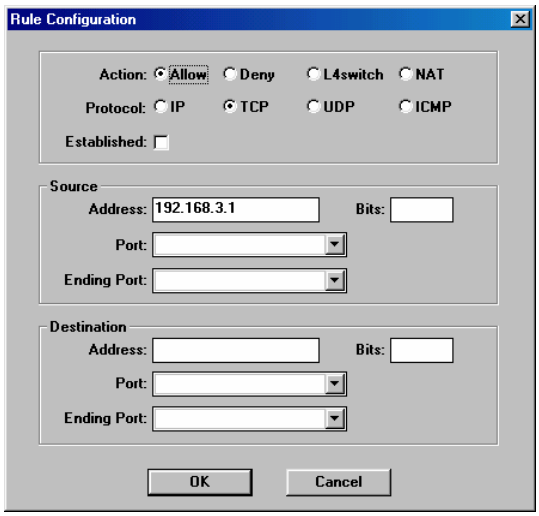

FIGURA -2.50- Cuadro de configuración de reglas particularizado

Dentro del cuadro de configuración de la regla se pulsa *"OK"* y ya está añadida la regla a la lista de reglas de nuestro filtro. Se vuelve a pulsar *"OK"*, esta vez dentro del cuadro de configuración del filtro y ya está el filtro añadido a la lista de filtros seleccionables.

Ahora falta aplicar el filtro a la interfaz *eth3* como filtro de salida, para ello, desde el cuadro de configuración de filtros para la interfaz *eth3*, escogiendo el filtro *F.Salidaeth3* del menú desplegable **Out Filter** tal y como se muestra en la figura 50.

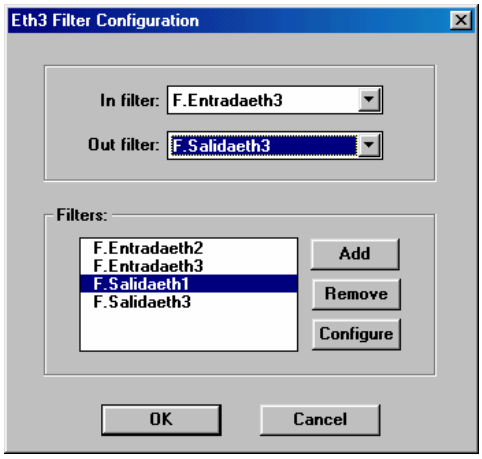

FIGURA -2.51- Cuadro de filtros relacionados con la interfaz *eth3*

Una vez llevada a cabo la puesta en marcha y configuración inicial de la unidad *Contivity 400*, creados los filtros y aplicados tal y como se ha especificado en este apartado, la unidad *Contivity 400* está configurada correctamente para funcionar como cortafuegos en la estructura de red especificada en este apartado, la cual proporciona una solución de seguridad según los requisitos previamente establecidos por la empresa. La unidad *Contivity 400* regulará, mediante los filtros aplicados a sus respectivas interfaces, el paso de los paquetes entre las distintas zonas de la arquitectura *Screened Subnet* permitiendo o rechazando el paso de los paquetes, según cumplan éstos o no unos requisitos previamente especificados, los cuales están orientados a dotar de una mayor seguridad a la red de la empresa ante el cualquier atacante que intente acceder a los equipos de su red interna, invadiendo de este modo la privacidad de la empresa.

Capítulo 3
VLAN

En diversas organizaciones, empresas o instituciones, tales como la UPCT, deben proporcionarse determinados servicios telemáticos a un número importante de usuarios. Si todos los usuarios accediesen a dichos servicios desde un puesto fijo y contasen con los mismos permisos de acceso, una configuración de la red corporativa "tradicional" sería adecuada. Sin embargo, la movilidad de los usuarios es grande y los servicios que demandan y a los que pueden acceder son muy diversos. En este caso, la arquitectura de red propuesta en este capítulo basada en la tecnología de Redes Virtuales Locales (VLAN) garantiza una mayor flexibilidad en el uso de la red. Cada grupo de trabajo (profesores, PAS, alumnos, e invitados) se identificará con una determinada VLAN. La tecnología VLAN realiza una distribución de los grupos a nivel lógico, por lo que dicha distribución es independiente de la localización física aumentado así la flexibilidad.

Para que el acceso a los grupos de trabajo se realice de manera segura, se ha optado por hacer uso del protocolo *Extensible Authentication Protocol Over LAN* (EAPOL) el cual está basado en el protocolo *Extensible Authentication Protocol* (EAP). El protocolo EAPOL trabaja conjuntamente con un servidor de autenticación RADIUS, el cual proporciona autenticación remota a los usuarios de los distintos grupos. A cada usuario se le pedirá un identificador de usuario y una clave antes de poder acceder a la VLAN que le corresponde. Para hacer todo esto del modo más flexible posible se ha va a hacer uso de la función de Asignación Dinámica de VLAN que proporciona el protocolo EAPOL. De esta forma, a partir de una serie de parámetros almacenados para cada usuario (en el servidor de autenticación) cuando un usuario sea autenticado, se le asignará automáticamente un identificador de VLAN. Esta característica permite a cualquier usuario conectarse a la VLAN que le corresponde sea cual sea su situación física e independientemente del equipo desde el cual realice la conexión, ya que la asignación de las VLAN se realiza basándose en el identificador de usuario y su clave. El servidor de autenticación permite también el almacenamiento de parámetros referentes al tipo de servicio que se va a ofrecer a un determinado usuario, en función de su identificador de usuario y su clave.

Para la resolución del problema planteado en este capítulo se van a usar los siguientes componentes:

- *Business Policy Switch 2000* (BPS 2000): Es el encargado de crear las VLAN y configurar la seguridad EAP para pedir autenticación de cualquier conexión a cualquiera de sus puertos. El BPS 2000 actúa de intermediario durante el proceso de autenticación entre el cliente y el servidor RADIUS tal y como se explicará mas adelante en el punto 3.2.3
- Cliente *Odyssey*: *Software* que será instalado en todas las máquinas cliente y que permitirá comunicarse con un servidor de autenticación RADIUS, en este caso a través del BPS.

- Servidor *FreeRADIUS*: Es el servidor de autenticación. Además de las tareas normales de autenticación se encargará de asignar a los usuarios a una VLAN determinada en función de los parámetros almacenados en el mismo.

3.1 VLAN

En este apartado se introducen los aspectos más relevantes de la tecnología VLAN así como sus diferentes tipos y aplicaciones. Dicha tecnología permite la asociación de un individuo, perteneciente a un determinado grupo de trabajo, con unos servicios a través de una red virtual.

3.1.1 Definición de VLAN

Las Redes de Área Local Virtuales (VLAN) son agrupaciones, definidas por *software*, de estaciones de trabajo que se comunican entre sí como si estuvieran conectadas al mismo segmento físico, incluso estando situadas en segmentos diferentes de una red de edificio o de campus por ejemplo. Es decir, la red virtual es una tecnología que permite separar la visión lógica de la red de su estructura física mediante el soporte de comunidades de intereses, con definición lógica, para la colaboración en sistemas informáticos de redes.

El concepto de red virtual simplifica el problema de administración de los movimientos, adiciones y cambios del usuario dentro de una empresa. Por ejemplo, si un departamento se desplaza a un edificio a través del campus, este cambio físico será transparente gracias a la visión lógica de la red virtual. Asimismo, se reduce notablemente el tiempo y los datos asociados con los movimientos físicos, permitiendo que la red mantenga su estructura lógica al coste de unas pocas pulsaciones del ratón del administrador de la red. Puesto que todos los cambios se realizan bajo control de *software*, los centros de cableado permanecen seguros y a salvo de interrupciones.

3.1.2 Tipos de VLAN

Basándose en las características que identifican a los miembros de la red virtual, pueden definirse cuatro tipos de VLAN:

- VLAN basadas en puertos.
- VLAN basadas en direcciones físicas o MAC.
- VLAN de capa 3 o basadas en protocolo.
- VLAN basadas en reglas.

3.1.2.1 VLAN basadas en puertos (*Membership by Port Group*)

Este tipo de VLAN consiste en la agrupación o asociación de varios puertos físicos pertenecientes a un solo conmutador o a varios. La asignación de los equipos a la VLAN se hace en base a los puertos a los que están conectados físicamente.

Muchas de las primeras implementaciones de las VLAN definían la pertenencia a la red virtual por grupos de puertos (por ejemplo, los puertos 1, 2, 3,7 y 8 de un determinado

un conmutador forman la VLAN A, mientras que los puertos 4,5 y 6 forman la VLAN B). Además, en la mayoría, las VLAN podían ser construidas sobre un único conmutador.

La segunda generación de implementaciones de VLAN basadas en puertos contempla la aparición de múltiples conmutadores (por ejemplo, los puertos 1 y 2 de un determinado conmutador 1 y los puertos 4, 5, 6 y 7 de otro determinado conmutador 2 podrían formar la VLAN A mientras que los puertos 3, 4, 5, 6, 7 y 8 del conmutador 1 combinados con los puertos 1, 2, 3 y 8 del conmutador 2 formarían la VLAN B).

La agrupación por puertos es todavía el método más común para definir la pertenencia a una VLAN, y su configuración es bastante sencilla.

La principal limitación a la hora de definir una VLAN basada en puertos es que el administrador de la red ha de reconfigurar la VLAN cada vez que un usuario se mueve de un puerto a otro. Este problema se soluciona con la aparición de una función denominada "Asignación Dinámica a VLAN", la cual es implementada por el *Business Policy Switch 2000* de *Nortel Networks*. Dicha función permite la asignación dinámica de un usuario a una determinada VLAN en función de su identificador de usuario y su clave.

3.1.2.2 VLAN basadas en direcciones físicas o MAC (*Membership by MAC address*)

Es el segundo escalón en la evolución de las VLAN. Trata de superar las limitaciones de las VLAN basadas en puertos. Operan agrupando estaciones finales en una VLAN en base a sus direcciones físicas o direcciones MAC. Este tipo de implementación tiene varias ventajas y desventajas.

Las VLAN basadas en direcciones MAC permiten a los administradores de la red el mover una estación de trabajo a una localización física distinta en la red y mantener su pertenencia a la VLAN. De este modo, las VLAN basadas en MAC pueden ser vistas como una VLAN orientada al usuario.

3.1.2.3 VLAN de capa 3 (Layer 3-Based VLAN)

Las VLAN de capa 3 tienen en cuenta el tipo de protocolo o las direcciones de la capa de red, para determinar la pertenencia a una VLAN.

Hay varias ventajas en definir VLAN de capa 3. En primer lugar, permite el particionado por tipo de protocolo, lo que puede ser de gran utilidad para decidir qué servicios o aplicaciones van a ofrecerse en cada VLAN. En segundo lugar, los usuarios pueden físicamente mover sus estaciones de trabajo sin tener que reconfigurar cada una de las direcciones de red de la estación (este es un beneficio principalmente para los usuarios de TCP/IP). Y en tercer lugar, definir una VLAN de capa 3 puede eliminar la necesidad de marcar las tramas para comunicar miembros de la red mediante conmutadores, reduciendo los gastos de transporte.

Una de las desventajas de definir la VLAN de capa 3 (al contrario de lo que ocurría en las dos anteriores) es su modo de trabajo. El inspeccionar direcciones de la capa 3 en paquetes consume más tiempo que buscar una dirección MAC en tramas. Por esta razón,

los conmutadores que usan información de la capa 3 para la definición de VLAN son generalmente más lentos que los que usan información de la capa 2.

3.1.2.4 VLAN basadas en reglas (*Policy Based VLAN).*

Este esquema es el más potente y flexible, ya que permite crear VLAN adaptadas a necesidades específicas de los gestores de red utilizando una combinación de reglas. Estas reglas pueden ser, por ejemplo, de acceso, con objeto de alcanzar unos ciertos niveles de seguridad en la red. Una vez que el conjunto de reglas que constituyen la política a aplicar a la VLAN se implementa, sigue actuando sobre los usuarios al margen de sus posibles movimientos por la red.

El BPS 2000 permite crear VLAN de los tres primeros tipos, basadas en puerto, dirección MAC o protocolo.

3.1.3 Aplicaciones de las VLAN

Las principales aplicaciones de una VLAN son:

Movilidad: Como hemos visto, el punto fundamental de las redes virtuales es el permitir la movilidad física de los usuarios dentro de los grupos de trabajo.

Dominios lógicos: Los grupos de trabajo pueden definirse a través de uno o varios segmentos físicos, o en otras palabras, los grupos de trabajo son independientes de sus conexiones físicas, ya que están constituidos como dominios lógicos.

Control y conservación del ancho de banda: Las redes virtuales pueden restringir los *broadcast* a los dominios lógicos donde han sido generados. Además, añadir usuarios a un determinado dominio o grupo de trabajo no reduce el ancho de banda disponible para el mismo, ni para otros.

Conectividad: Los modelos con funciones de *routing* nos permiten interconectar diferentes conmutadores y expandir las redes virtuales a través de ellos, incluso aunque estén situados en lugares geográficos diversos.

Seguridad: Los accesos desde y hacia los dominios lógicos, pueden ser restringidos, en función de las necesidades específicas de cada red, proporcionando un alto grado de seguridad.

Protección de la inversión: Las capacidades VLAN están, por lo general, incluidas en el precio de los conmutadores que las ofrecen, y su uso no requiere cambios en la estructura de la red o cableado, sino más bien los evitan, facilitando las reconfiguraciones de la red sin costes adicionales

3.2 Seguridad

Es importante que cada individuo o máquina perteneciente a un grupo de trabajo sólo pueda acceder a aquellos servicios para los que está autorizado. Por lo tanto, en la

arquitectura que se va a proponer, la seguridad en control de acceso es un objetivo importante.

El encargado de proporcionar, en este proyecto, dicho control de acceso es el BPS 2000. Tres son las opciones que el BPS 2000 ofrece en cuanto a la seguridad en el control de acceso se refiere:

- Seguridad basada en RADIUS.
- Seguridad basada en MAC.
- Seguridad basada en EAPOL.

3.2.1 Seguridad basada en RADIUS

Permite restringir el acceso a la administración del conmutador mediante autenticación remota de usuario usando el protocolo de seguridad *Remote Authentication Dial-In User Services* (RADIUS).

El protocolo funciona del siguiente modo: en el servidor RADIUS se almacenan una serie de ficheros de configuración donde se especifican todos los parámetros referentes tanto al servidor como a los usuarios que podrán acceder al mismo. En uno de esos ficheros se incluyen una serie de entradas correspondientes cada una de ellas a un determinado usuario. Las entradas de este fichero asocian a un usuario con su correspondiente clave y una serie de atributos tales como el tipo de servicio o el tipo de autenticación. El cliente envía su identificador de usuario y su clave, tras la autenticación, siempre y cuando el resultado de la misma haya sido positivo, el cliente podrá acceder a los servicios detallados para él en el servidor RADIUS.

En el caso concreto del BPS 2000, pueden proporcionarse dos modos distintos de acceso al mismo según el valor del parámetro *Service-Type* almacenado en el servidor de autenticación:

- Para proporcionar acceso de sólo lectura al conmutador el valor del atributo *Service-Type* ha de fijarse como *NAS-Prompt*.
- Para que el usuario acceda al conmutador en modo lectura/escritura, el valor de *Service-Type* debe ser *Administrative*.

3.2.2 Seguridad basada en MAC

La seguridad basada en direcciones físicas o direcciones MAC establece un control de acceso en función de unas determinadas listas donde se especifican una serie de direcciones MAC, origen o destino, permitidas.

En el caso del BPS 2000, éste permite crear dos listas de direcciones MAC:

- Una lista de hasta diez direcciones MAC destino que se deseen filtrar. Todos los paquetes con cualquiera de las direcciones MAC contenidas en la lista serán rechazados, sin importar la dirección MAC origen, ni el puerto de ingreso, ni la VLAN a la que pertenezca.

- Una lista de hasta 448 direcciones MAC origen que serán las que tendrán acceso al conmutador.

3.2.3 Seguridad basada en EAPOL

Esta es la opción que va a usarse para resolver el problema de la seguridad en el acceso, en función de los grupos de trabajo, a los grupos en este proyecto. También se hará uso de la función de Asignación Dinámica de VLAN que proporciona el protocolo EAPOL para proporcionar una mayor flexibilidad en el acceso de los usuarios a las distintas VLAN.

3.2.3.1 Seguridad EAPOL

El esquema de seguridad EAPOL permite el intercambio de información de autenticación entre cualquier equipo conectado al conmutador y un servidor de autenticación, como por ejemplo un servidor RADIUS. *Extensible Authentication Protocol Over LAN* (EAPOL) se basa en el protocolo EAP tal y como se especifica en el Draft IEEE P802.1X para permitir establecer controles de acceso entre redes LAN.

Como ya se ha comentado anteriormente, la seguridad basada en el protocolo EAP actúa conjuntamente con un servidor RADIUS para extender los beneficios de la autenticación remota a los usuarios de redes LAN .

A continuación se explica mediante un ejemplo como el BPS 2000 configurado con seguridad basada en EAP reacciona ante una conexión:

- El conmutador detecta una nueva conexión a uno de sus puertos.
  - El conmutador envía una petición de identificador de usuario al nuevo cliente.
  - EAPOL encapsula el identificador de usuario y lo envía al servidor RADIUS.
  - El servidor RADIUS responde con una petición de clave para el usuario.
- El cliente envía un clave encriptado al conmutador dentro de un paquete EAP.
  - El conmutador reenvía el paquete EAPOL al servidor RADIUS.
  - Si el servidor RADIUS valida la clave, al nuevo usuario le es permitido el acceso al conmutador y a la red.

Algunos de los términos y componentes usados en la seguridad basada en EAP son los siguientes:

- Cliente: Es la máquina que solicita el acceso a la red.
- Autenticador: *Software* con el único propósito de autorizar a un determinado cliente. Se comunica con el cliente usando el protocolo de encapsulación EAPOL.
- Servidor de autenticación: un servidor RADIUS que proporciona servicios de autorización al autenticador.
- PAE (Port Access Entity): Entidad *software* asociada con cada puerto que soporta funcionalidad tanto de cliente como de autenticador. Para el caso del BPS el PAE del autenticador reside en el propio conmutador.

- Puerto controlado: Cualquier puerto del conmutador que tenga activada la característica de seguridad basada en EAP.

El autenticador se encarga de decidir cuál debe ser el estado (modo de funcionamiento) del puerto controlado. Dicho estado puede variar entre dos opciones:

- Reenvío o *Forwarding*: estado en el que se permite el paso de los paquetes a través del conmutador mediante el puerto en cuestión.
- Bloqueo o cerrado: no se permite el paso de paquetes a través de dicho puerto
-

El autenticador actúa para cada puerto controlado en el conmutador.

Durante la inicialización del sistema o, inicialmente, cuando un cliente se conecta a un puerto controlado del conmutador, el estado por defecto del puerto es bloqueado. El puerto permanece en este estado mientras el autenticador procesa los paquetes EAP y el resto de información necesaria para decidir si se permite o no el reenvío de paquetes. El autenticador facilita el intercambio de información de autenticación entre el cliente y el servidor de autenticación encapsulando el paquete EAP dentro de de una trama RADIUS antes de enviarlo al servidor de autenticación.

Cuando el servidor de autenticación devuelve un mensaje de “éxito” o “fallo” tras el proceso de autenticación, el estado del puerto controlado cambia de acuerdo con dicho mensaje. Si la autorización es permitida, el estado del puerto cambia a reenvío o *forwarding*. En caso contrario el estado del puerto dependería del valor asignado al campo de control de tráfico en la configuración de la seguridad EAPOL.

El campo del control de tráfico puede tener uno de los dos valores siguientes:

- entrante y saliente: si el puerto controlado es desautorizado, las tramas no se transmiten a través del puerto; todas las tramas recibidas en el puerto controlado se descartan. El estado del puerto controlado cambia a bloqueo.
- entrante: si el puerto controlado es desautorizado, las tramas recibidas en el puerto se descartan, pero las tramas salientes son enviadas a través del puerto.

3.2.3.2 Asignación dinámica de VLAN mediante EAPOL

Se trata de una función de reciente aparición que se aplica a las VLAN basadas en puertos, dotando a éstas de una mayor flexibilidad Esta característica permite, en un sistema que use seguridad EAPOL y, siempre y cuando el resultado de la autenticación sea positivo, asignar dinámicamente los usuarios a las VLAN. Dicha asignación dinámica se realiza mediante una serie de parámetros previamente almacenados (basados en el identificador de usuario) en un servidor de autenticación. El cual, una vez realizada la autenticación, con resultado positivo, informa al conmutador sobre en qué VLAN debe quedar encuadrado el usuario en cuestión.

Los siguientes valores de configuración VLAN se ven afectados:

- *Port membership*: Específica los puertos que son miembros de una determinada VLAN.
- PVID: Identifica a un puerto con una VLAN específica.
- Prioridad del puerto: Indica el nivel de prioridad de las tramas no marcadas (*untagged frames*) recibidas en un determinado puerto.

Cuando la seguridad EAPOL es desactivada en un puerto que ha sido previamente autorizado y cuya configuración VLAN ha sido cambiada, dicha configuración es restaurada directamente desde la memoria no volátil de acceso aleatorio (NVRAM) del conmutador.

Los valores de la configuración VLAN asignados dinámicamente por EAPOL no son almacenados en la memoria NVRAM del conmutador.

El servidor de autenticación RADIUS permite configurar parámetros específicos de miembros VLAN y prioridad del puerto para cada usuario.

Cuando un usuario intenta entrar en un sistema que ha sido configurado para autenticación EAPOL el servidor de autenticación reconoce su identificador de usuario, entonces, notifica al conmutador unos determinados valores, específicos de dicho usuario (previamente configurados en el servidor de autenticación) que le permiten establecer a que grupo (*membership*) va a pertenecer, así como el PVID que tiene asignado.

3.3 RADIUS

Para la realización del ejercicio planteado en este capítulo se hace uso de un servidor de autenticación mediante el protocolo RADIUS (*Remote Authentication Dial-In User Services*) combinando con el uso del protocolo de seguridad EAPOL. En este apartado se introducen las nociones básicas sobre el funcionamiento del protocolo RADIUS tanto en la parte de cliente como en la parte del servidor. En el caso específico de este proyecto va a usarse el servidor RADIUS de libre distribución *FreeRADIUS*, en concreto, va a usarse la última versión disponible en el momento de la realización del proyecto para el sistema operativo Linux.

3.3.1 Protocolo RADIUS

RADIUS es un protocolo de uso ampliamente extendido que permite la autenticación, la autorización, y la contabilidad centralizadas para el acceso de red. Desarrollado originalmente para acceso remoto *dial-up* (marcado manual), RADIUS es ahora soportado por servidores VPN (*Virtual Private Networks*), puntos de acceso inalámbricos, conmutadores de autenticación de *Ethernet*, acceso DSL (*Digital Suscriber Line*) y otros tipos de redes de acceso. El protocolo RADIUS se describe en la RFC 2865, "*Remote Authentication Dial-In User Service* (RADIUS),"(IETF *Draft* Estándar) y la RFC 2866 "*RADIUS Accounting*" (Informativa).

Un cliente RADIUS (normalmente un servidor de acceso envía las credenciales de usuario y la información de los parámetros de conexión en forma de mensaje RADIUS al servidor RADIUS. El servidor RADIUS comprueba las credenciales del cliente, indicando mediante un mensaje de respuesta si se autoriza o no la petición del cliente RADIUS. El cliente RADIUS también puede enviar al servidor RADIUS mensajes de contabilidad (*Accounting*). Adicionalmente, el estándar RADIUS soporta el uso de *proxies* RADIUS. Un *proxy* RADIUS es un computador que remite mensajes RADIUS entre clientes RADIUS, servidores RADIUS u otros *proxies* RADIUS. Los mensajes RADIUS nunca se envían entre el cliente de acceso y el servidor de acceso.

Los mensajes RADIUS son enviados como mensajes UDP (*User Datagram Protocol*). El puerto UDP 1812 es usado para los mensajes RADIUS de autenticación y el puerto UDP 1813 es usado para los mensajes RADIUS de contablidad. Algunos servidores de acceso usan el puerto UDP 1645 para los mensajes RADIUS de

autenticación y el puerto 1646 para los mensajes RADIUS de contabilidad. Sólo un mensaje RADIUS se incluye en la carga útil UDP de un paquete RADIUS.

Las RFCs 2865 y 2866 definen los siguientes tipos de mensajes RADIUS:

- ***Access-Request***: Enviado por el cliente RADIUS para pedir autenticación y autorización para un intento de conexión a la red de acceso.
- ***Access-Accept***: Enviado por el servidor RADIUS en respuesta a un mensaje *Acces-Request*. Este mensaje informa al cliente RADIUS que ha sido autenticado.
- ***Access-Reject***: Enviado por el servidor RADIUS en respuesta a un mensaje *Acces-Request*. Este mensaje informa al cliente RADIUS que el intento de conexión ha sido rechazado. Un servidor RADIUS envía este mensaje si las credenciales no son autenticas o el intento de conexión no es autorizado.
- ***Access-Challenge***: Enviado por el servidor RADIUS en respuesta a un mensaje *Acces-Request*. Este mensaje es un mensaje de "desafío" (*challengue*) para el cliente RADIUS que requiere una respuesta.
- ***Accounting-Request***: Enviado por el cliente RADIUS para especificar la información de contabilidad de una conexión que fue aceptada.
- ***Accounting-Response***: Enviado por el servidor RADIUS en respuesta a un mensaje *Accounting-Request*. Este mensaje reconoce la recepción correcta del mensaje *Accounting-Request* y del proceso del mismo.

Un mensaje RADIUS consiste en una cabecera y unos atributos. Cada atributo específica una parte de la información acerca del intento de conexión. Por ejemplo, hay un atributo para el identificador de usuario, la clave del usuario, el tipo de servicio demandado por el usuario, y la dirección IP del servidor de acceso. Los atributos se utilizan para transportar la información entre los clientes, *proxies* y servidores. Por ejemplo, la lista de atributos en un mensaje *Access-Request* incluye información acerca de las credenciales del usuario y los parámetros del intento de la conexión. En cambio, la lista de mensajes de un mensaje *Access-Accept* incluye información acerca del tipo de conexión que puede llevarse a cabo, la prioridad de la conexión y cualquier atributo específico del vendedor (VSAs).

Los atributos están definidos en las RFCs 2865, 2866, 2867, 2868, 2869 y 3162. RFCs y "drafts" de Internet definen atributos RADIUS adicionales.

Para proporcionar seguridad para los mensajes RADIUS, el cliente y el servidor RADIUS están configurados con un secreto común compartido. El secreto compartido es usado para dar seguridad al tráfico RADIUS y y se configura comúnmente como una secuencia de texto en el cliente y el servidor RADIUS.

3.3.2 EAP sobre RADIUS

EAP sobre RADIUS no es un tipo del protocolo EAP, sino que consiste en el paso de los mensajes EAP por un servidor de acceso remoto a un servidor RADIUS para la autenticación. Un mensaje enviado entre el cliente y el servidor de acceso se ajusta a un formato de atributos RADIUS mensaje EAP y se envía en un mensaje RADIUS entre el servidor de acceso y el servidor RADIUS. El servidor de acceso se convierte en un dispositivo de paso que reenvía mensajes EAP entre el cliente y el servidor RADIUS. El proceso de los mensajes EAP ocurre en el cliente y el servidor RADIUS no en el servidor

de acceso, éste lo único que hace es adaptar los mensajes EAP al formato del protocolo RADIUS para posteriormente enviarlos al servidor de autenticación.

En un uso frecuente de EAP sobre RADIUS, el servidor de acceso se configura para usar EAP y para usar RADIUS como proveedor de autenticación. Cuando se realiza un intento de conexión el cliente negocia el uso de EAP con el servidor de acceso. Cuando el cliente envía un mensaje EAP al servidor de acceso, éste lo encapsula en un mensaje RADIUS y lo envía al servidor RADIUS que tenga configurado. El servidor RADIUS procesa el mensaje EAP y responde mandando un paquete RADIUS ajustado a formato EAP al servidor de acceso, entonces éste envía el mensaje EAP al cliente.

3.4 Desarrollo del ejercicio “VLAN Dinámicas”

En este apartado se plantea el problema a resolver así como la configuración de las distintas partes que intervienen en dicho ejercicio para su correcta resolución.

3.4.1 Planteamiento del problema

La problemática que se plantea es la siguiente: en la UPCT hay distintos grupos de usuarios: profesores, alumnos, PAS. Cada uno de estos grupos debe tener acceso a unos servicios determinados. Se pretende que los usuarios de cada grupo puedan tener acceso a sus correspondientes servicios independientemente de la situación física donde se encuentren. Para conseguir esto, en este proyecto se ha decidido hacer uso de la tecnología *Virtual Local Area Network* (VLAN) de modo que cada grupo se incluya en una red virtual determinada, de forma que la distribución se hace a nivel lógico, por lo que es independiente de la situación física del usuario.

De acuerdo con los diferentes grupos que podemos encontrar, la distribución por VLAN sería:

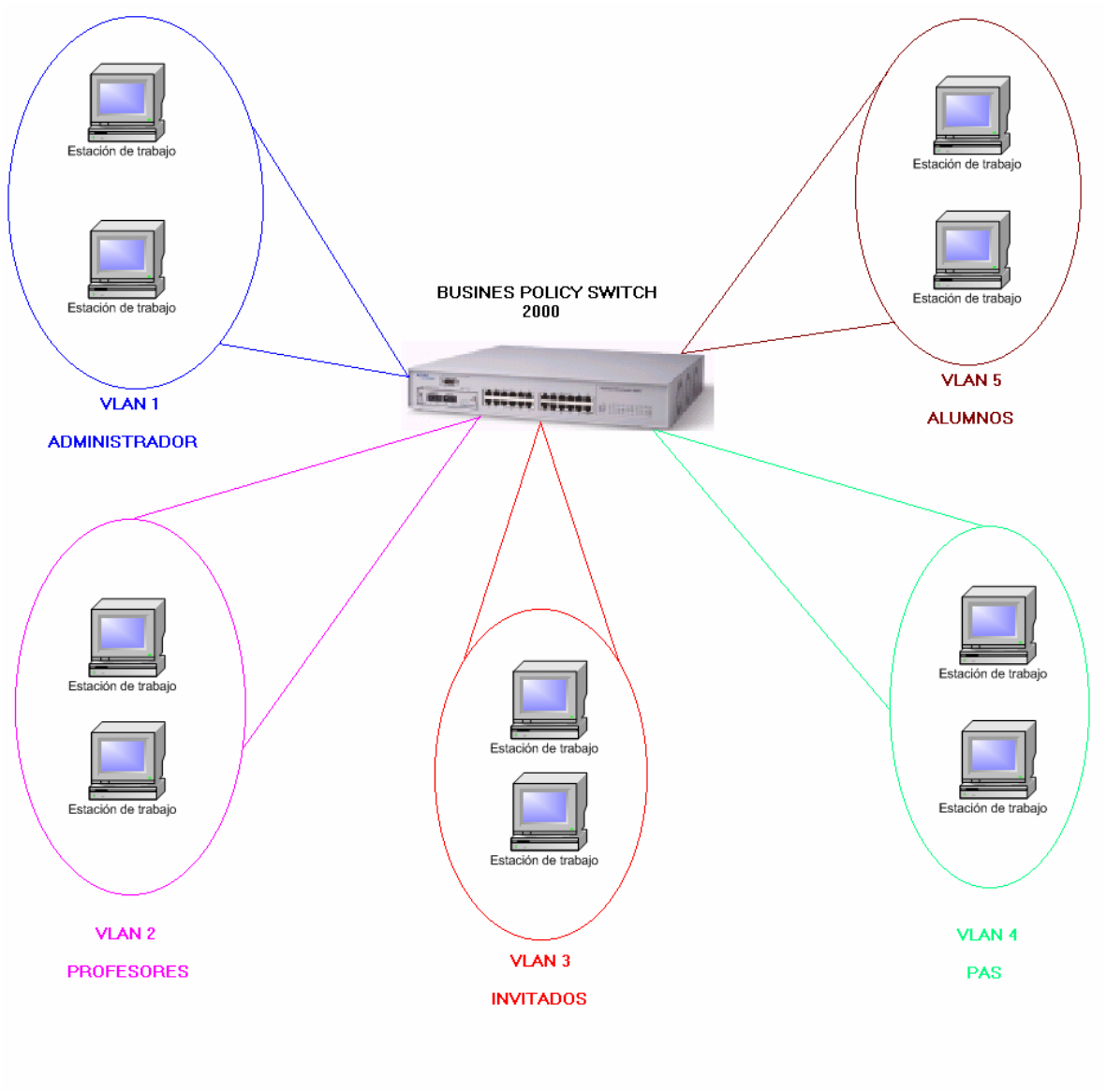

Figura -3.1- Esquema de red para la resolución del ejercicio propuesto

- **VLAN1**: Administrador. Red lógica que se va a definir como "Management Vlan", es decir, como la VLAN desde la que se puede administrar el conmutador BPS 2000.

- **VLAN2**: Profesores. Red local lógica en la que se ubican todos los miembros del profesorado de la universidad.

- **VLAN3**: Invitados. Red local lógica en la que se situará cualquier usuario "invitado" que se conecte al Business Policy Conmutador 2000.

- **VLAN4**: PAS. Red local lógica compuesta por los miembros del Personal de Administración y Servicios (PAS).

- **VLAN5**: Alumnos. Red local lógica compuesta en su totalidad por alumnos.

Se desea dar flexibilidad de acceso a las VLAN, a su vez manteniendo el grado de seguridad que se tendría si cada tipo de usuario sólo pudiese acceder a la red desde determinados puntos o rosetas. Para ello se va a usar el protocolo EAPOL del estándar 802.1x, en combinación con un servidor de autenticación RADIUS (*FreeRADIUS*).

Dentro de las características de EAPOL se hará uso de *Dynamic VLAN assigment*, que permite la asignación dinámica de los usuarios a las distintas VLAN en función de su identificador de usuario y su clave, para asignar a cada usuario a su VLAN correspondiente. Para poder hacer uso de esta característica las VLAN creadas deben ser basadas en puertos, al menos en el *Business Policy 2000*. Por tanto a cada usuario se le exigirá que se autentique al conectarse físicamente a la red. Dicha autenticación será llevada a cabo por un servidor RADIUS. Según el resultado obtenido se permitirá o denegará el acceso al usuario. En caso de serle permitido, se le encaminará de manera automática a una determinada VLAN, en función de los parámetros almacenados para el usuario en cuestión en el servidor de autenticación. Todos los datos referentes a los usuario y a la VLAN correspondiente a cada uno, son almacenados en el servidor RADIUS tal y como se explicó en el apartado 3.2.3.2.

Por último, también se desea proteger la interfaz Web de administración del BPS 2000 mediante autenticación a través de un servidor RADIUS.

A continuación, se describe la configuración de los tres componentes que van a ser utilizados para cumplir correctamente con los requisitos planteados por el ejercicio, que son el conmutador *Business Policy Switch 2000*, el cliente EAP *Odyssey* y el servidor de autenticación *FreeRADIUS*.

3.4.2 Servidor RADIUS

En este apartado van a describirse tanto la instalación como la configuración del servidor RADIUS para la resolución del ejercicio propuesto. Así mismo, se describirá también como comprobar el correcto funcionamiento del servidor RADIUS antes de hacerlo funcionar dentro del esquema que da solución al ejercicio.

3.4.2.1 Instalación

En primer lugar se descarga el archivo *FreeRADIUS.tar.gz* desde la Web oficial del *FreeRADIUS* www.FreeRADIUS.org de forma totalmente gratuita. Se descarga la versión para Linux, que será el sistema operativo bajo en cual se va a poner en funcionamiento el servidor RADIUS. Concretamente, para este proyecto en particular se ha usado la versión 0.9.2 del *software* última versión disponible en el momento de la realización del proyecto.

Una vez se ha descargado el archivo se procede a la instalación del *software* mediante la siguiente secuencia de comandos:

```
1. tar -zxvf FreeRADIUS.tar.gz
2. ./configure
3. ./configure --localstatedir=/var --sysconfdir=/etc
4. make
5. make install
```

La funcionalidad de cada uno de los comandos de la secuencia de instalación es la siguiente:

1. Descompresión de los ficheros fuente.
2. Mediante es comando se realiza la compilación de *FreeRADIUS*. Antes de ejecutar este comando es necesario asegurarse de que en el equipo en el que se va a ejecutar el servidor se han instalado previamente las aplicaciones *gcc*, *glibc*, *binutils* y *gmake*. Una vez comprobado, desde el directorio donde se han descomprimido los ficheros fuente se ejecuta el comando y comienza la compilación.
3. Este comando acompañado de las dos opciones indicadas, permite especificar cuál será la ubicación de los ficheros de configuración y de los ejecutables.
4. Mediante este comando se generan los ficheros binarios.
5. Con este comando se colocan los archivos en las localizaciones adecuadas (localizaciones comunes para la mayoría de servidores RADIUS que serán vistas más adelante) y además instalará también archivos de configuración si la máquina sobre la que se esta ejecutando no ha tenido antes un servidor RADIUS instalado. En caso de que ya hubiese habido un servidor RADIUS instalado en la máquina el procedimiento no sobrescribirá la configuración existente e informará acerca de los archivos que no se instalaron.

Una vez terminada la secuencia de comandos, el servidor RADIUS se encuentra correctamente instalado para comenzar a ser configurado para las necesidades específicas del ejercicio.

3.4.2.2 Ficheros de configuración

Una vez finalizado el proceso de instalación, antes de poder usar el servidor es necesario modificar algunos ficheros de configuración.

Los ficheros de configuración del servidor RADIUS están situados en el directorio:

```
/etc/raddb
```

Tal y como se ha configurado durante la instalación de los mismos.

Normalmente, la distribución de los ficheros está estructurada de la siguiente manera en la mayoría de productos RADIUS:

Ficheros ejecutables

```
/usr/local/bin and /usr/local/sbin
```

Ficheros de documentación y ayuda

```
/usr/local/man
```

Ficheros de configuración

```
/etc/raddb
```

Ficheros de incidencias

/var/log and /var/log/radacct

Los ficheros de configuración de mayor relevancia son los siguientes:

- **clients.conf**: En este fichero se guarda una lista de las máquinas que pueden actuar como clientes del servidor RADIUS.
- **users**: Fichero donde se almacenan una serie de entradas, cada una de ellas correspondientes a un usuario y en la que se especifican una serie de parámetros concretos para dicho usuario.
- **radius.conf**: En él se configuran las opciones referentes al propio servidor RADIUS, tales como por ejemplo el método de encriptación utilizado.

De los ficheros mencionados anteriormente, el único que va a ser configurado para la resolución del problema planteado en este proyecto es el fichero de configuración ***users***. En dicho archivo se incluyen todos los usuarios que pueden acceder el servidor RADIUS (a excepción de los usuarios con cuentas locales en la máquina en la que se está ejecutando el servidor), pudiendo especificarse multitud de parámetros para cada uno de ellos, tales como el tipo de autentificación, tipo de servicio, clave. A continuación se muestra un ejemplo de una entrada del fichero ***users***:

```
User1      Auth-Type := Local, User-Password == "passuser"
       Service-Type = Administrative-User,
```

En el ejemplo se identifica al usuario con identificador "user1" cuya clave es "passuser" y que al autenticarse tendrá acceso al sistema como administrador del mismo.

3.4.2.3 Configuración del servidor RADIUS

Para cumplir los requisitos planteados por el ejercicio propuesto se configurará el fichero ***users*** con las siguientes entradas:

```
prof1  Auth-Type := EAP, User- Password == "prof1pass"
       Service-Type = Administrative-User,
       Tunnel-Type = 13,
       Tunnel-Medium-Type = 6,
       Tunnel-Private-Group-Id = 1


invit1 Auth-Type := EAP, User-Password == "invit1pass"
       Service-Type = Administrative-User,
       Tunnel-Type = 13,
       Tunnel-Medium-Type = 6,
       Tunnel-Private-Group-Id = 2


Pas1   Auth-Type := EAP, User- Password == "pas1pass"
       Service-Type = Administrative-User,
```

```
        Tunnel-Type = 13,
        Tunnel-Medium-Type = 6,
        Tunnel-Private-Group-Id = 3


alum1   Auth-Type := EAP, User- Password == "alum1pass"
        Service-Type = Administrative-User,
        Tunnel-Type = 13,
        Tunnel-Medium-Type = 6,
        Tunnel-Private-Group-Id = 4


admin1  Auth-Type := EAP, User- Password == "admin1pass"
        Service-Type = Administrative-User,
        Tunnel-Type = 13,
        Tunnel-Medium-Type = 6,
        Tunnel-Private-Group-Id = 5
```

La configuración, exceptuando el nombre de usuario y la clave, es prácticamente la misma para todos los usuarios definidos, excepto el atributo *Tunnel-Private-Group-Id* que indica a que VLAN es asignado el usuario cuando es autenticado por el servidor RADIUS. Se describen a continuación éste y otros atributos asignados a los usuarios:

- *Auth-Type*: Indica el tipo de autentificación para un determinado usuario. En el caso que se plantea se le asigna *"EAP"*, lo que quiere decir que el usuario va a ser autenticado usando el protocolo EAP. Otros posibles valores para el tipo de autenticación son *"System"*, que indica que el usuario es un usuario de una cuenta local de la máquina donde se está ejecutando el servidor RADIUS, y *"Local"* que indica que la autentificación del usuario es local a la máquina cliente, lo que quiere decir que busca al usuario así como su clave para ser autenticado en el archivo de configuración ***users***.
- *Tunnel-Type*: Este atributo indica el protocolo de *tunneling* especificado para un determinado usuario, en este caso se le asigna a todos los usuarios el valor "13", lo que indica que el tipo de túnel es VLAN.
- *Tunnel-Medium-Type*: Es un valor numérico que indica el medio de transporte a utilizar al crear un túnel basado en protocolo que soporta múltiples tipos de túneles. En este caso se le asigna el valor "6" que indica que se va a usar la norma IEEE 802.
- *Tunnel-Private-Group-Id*: Como se ha citado anteriormente, éste atributo es usado para identificar una VLAN determinada, que es a la que es asignado el usuario cuando es autenticado por el servidor RADIUS. Por ejemplo, *prof1* pertenece a la VLAN 1, por lo que el valor del atributo Túnel-Private-Group-Id para este caso es igual a 1.

La configuración del *script* **users** no está del todo finalizada, ya que se va a proteger la interfaz Web de administración del conmutador y el acceso por *telnet* mediante autenticación a través de un identificador de usuario y su correspondiente clave almacenados también en un servidor RADIUS. Para ello se añaden dos nuevos usuarios a la lista de usuarios del fichero ***users***, dicho usuario va a ser un usuario con privilegios administrativos para de este modo poder acceder a la interfaz Web de configuración del

conmutador y cambiar la configuración de éste a su antojo. La entrada que se añade al fichero ***users*** es la siguiente:

```
administ    Auth-Type := EAP, User-Clave =="administpass"
       Service-Type = Administrative-User,
       Tunnel-Type = 13,
       Tunnel-Medium-Type = 6,
       Tunnel-Private-Group-Id = 5


adminSys    Auth-Type := Local, User-Clave == "passadminSys"
       Service-Type = Administrative-User,
```

3.4.2.4 Puesta en marcha del servidor RADIUS

Una vez configurado y verificado el correcto funcionamiento del servidor RADIUS (ver apéndice A), se procede a su puesta en marcha, para lo que una vez dentro del directorio

```
/usr/local/sbin/
```

Se ejecuta el siguiente comando:

```
./radiusd –X –p 1645
```

Para realizar la ejecución de este comando se necesita ser el usuario “root” del sistema.

Se añaden los siguientes parámetros al comando *radiusd*:

- -X: con este parámetro se ejecuta el servidor en modo debuging, de tal modo que pueden observarse los mensajes intercambiados entre el servidor y los clientes, así como el contenido de los mismos.
- -p 1645: De este modo se fija como puerto sobre el que se ejecuta el servidor al puerto 1645. Se hace esto debido a que por norma general la mayoría de productos RADIUS usan el puerto 1645 como puerto por defecto para el servidor RADIUS.

3.4.3 Cliente EAP

3.4.3.1 Configuración cliente EAP

Una vez instalado el programa desde el icono de la barra de tareas o bien desde el acceso directo en el menú *Inicio -> Programas -> Funk Software -> Odyssey Client -> Odyssey Client Manager* se arranca el *Client Manager*, programa que permite configurar el cliente EAP (En el apéndice B se incluye una descripción breve del cliente *Odyssey* en

la que se explican las principales opciones de configuración, para facilitar su uso). Lo primero es desactivar el cliente mediante la opción *Settings -> Disable Odyssey* y una vez hecho esto comenzar su configuración.

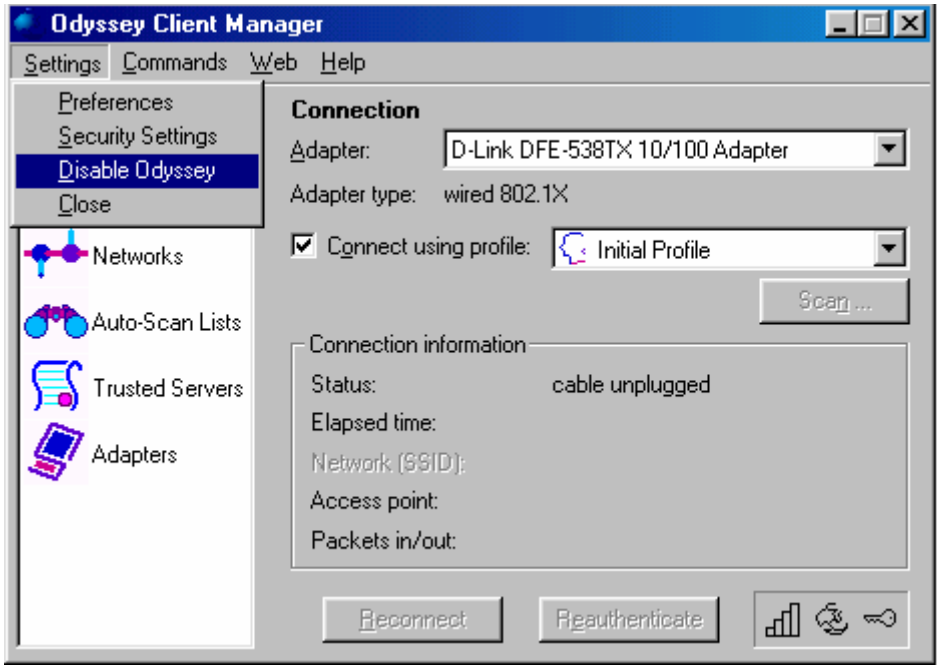

Figura -3.2- Ventana de configuración de la conexión del cliente *Odyssey*

El primer apartado a configurar es el de los perfiles de usuario. Para ello se usa la opción *Profiles*. A continuación se muestra un ejemplo de creación de perfil de usuario para el usuario "*profesor1*", el resto de perfiles ser crearían de idéntica forma excepto parámetros como el nombre de usuario o la clave.

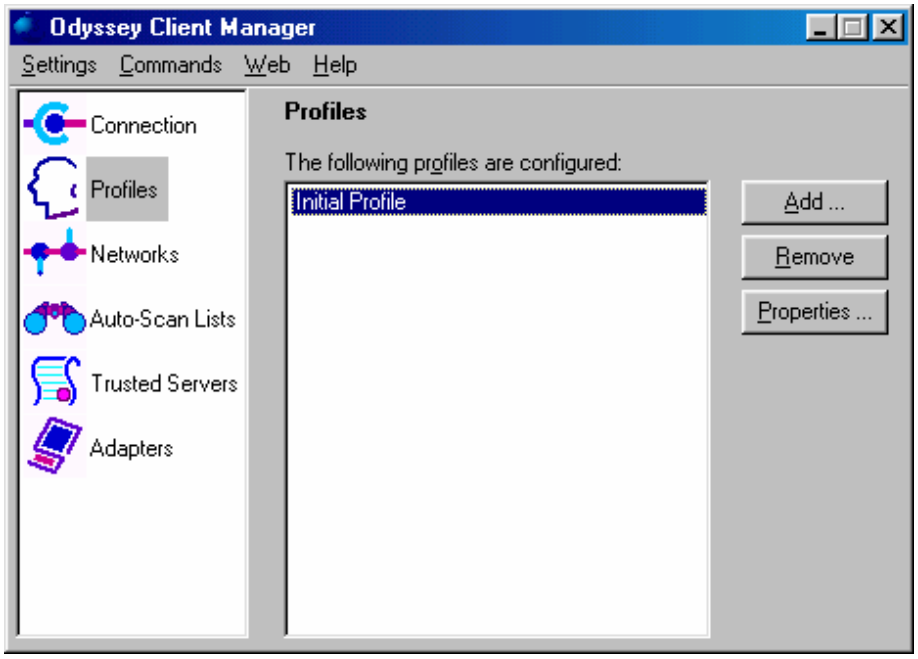

Figura -3.3- Ventana de configuración de perfiles de usuario del cliente *Odyssey*

Como puede observarse, inicialmente en la lista de perfiles aparece únicamente el perfil creado por defecto denominado *Inicial Profile*. Pulsando el botón *Add* se entra en el menú de creación del perfil de usuario.

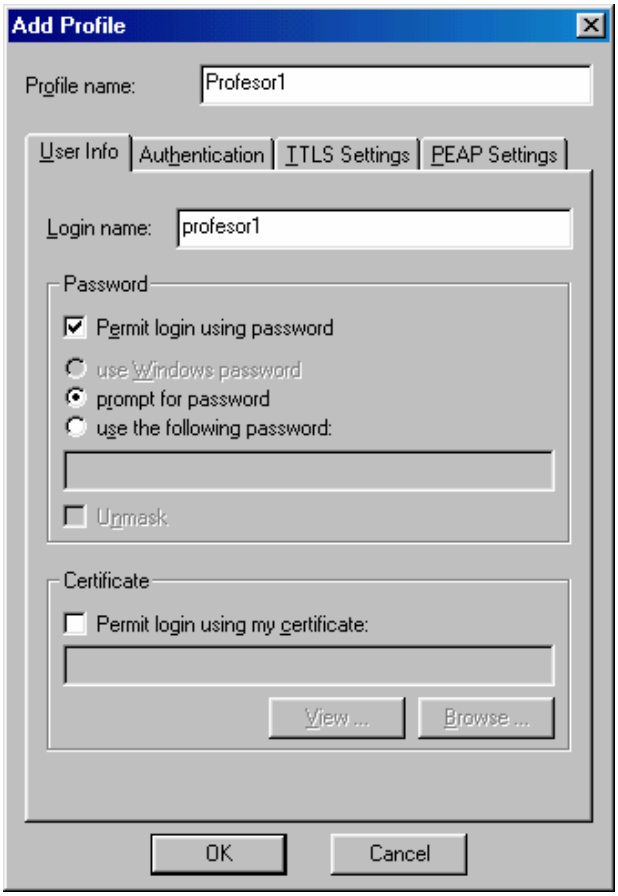

Figura -3.4- Ventana de información de usuario del cliente *Odyssey*

En dicho menú se configura en la pestaña *User Info* como nombre de usuario, es decir como *Login name*, “profesor1” y como nombre del perfil (*Profile name*) “Profesor1”. Si no están activadas las casillas *Permit login using clave* y *prompt for clave* se activarán, permitiendo de esta manera el acceso mediante un clave donde dicho clave se introducirá en una ventana mostrada por el programa en la que se pide

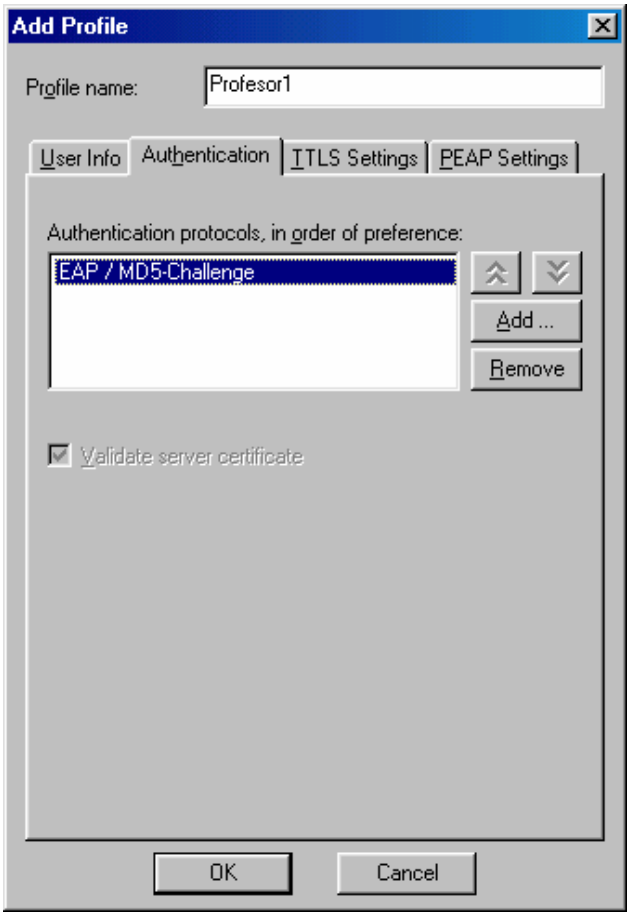

Figura -3.5- Ventana desde donde se configura los tipos de encriptación que usará un determinado usuario para el intercambio de mensajes

dicha clave. Dentro de la pestaña *Authentication* se eliminan todos los protocolos de autenticación de la lista y se pulsa el botón *Add* para añadir un nuevo

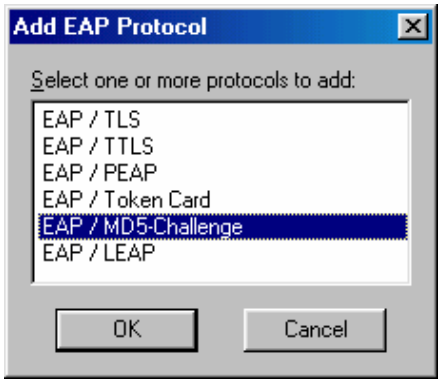

Figura -3.6- Cuadro de diálogo donde se selecciona un determinado método de encriptación

protocolo a la lista, la opción a escoger es *EAP/MD5-Challengue* de modo que el método de encriptación usado para el intercambio de mensajes entre cliente y servidor sea MD5. Este método es el que usa el BPS 2000 para la encriptación de los mensajes, además, es el método por defecto del servidor *FreeRADIUS*, por lo que no será necesario configurarlo en el mismo. Se pulsa *"OK"* y ya está creado y añadido a la lista de perfiles el perfil *profesor1*.

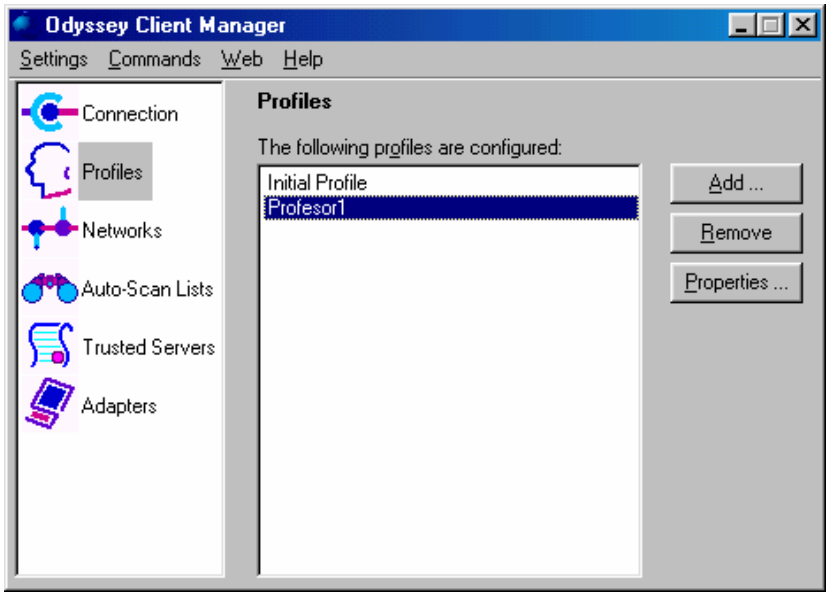

Figura -3.7- Ventana de perfiles de usuario con el perfil *Profesor1* añadido a la lista de perfiles disponibles

La siguiente opción a configurar del cliente EAP es la opción *Networks*, donde se configuran las redes para las que está configurado el cliente EAP. Se dejará la

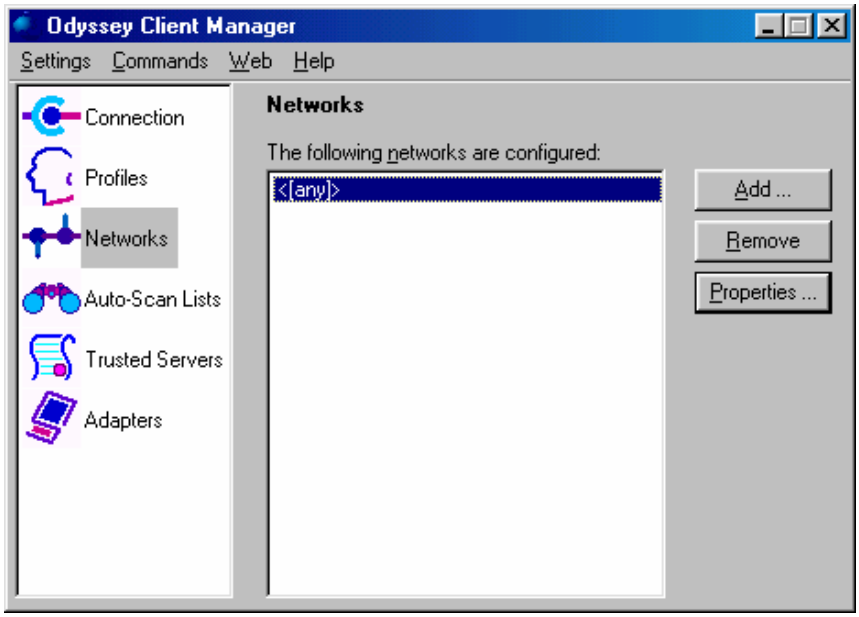

Figura -3.8- Ventana de configuración de las redes a las que afectará el cliente *Odyssey*

opción por defecto, que es la red denominada *any*, pero cambiando una serie de parámetros de dicha opción. Para ello se marca la red y se pulsa el botón *Properties*.

Dentro de este menú se activan las casillas *Connect to any avaliable network* y *Autentícate using profile*, en ésta última se elige el perfil con el que se quiere

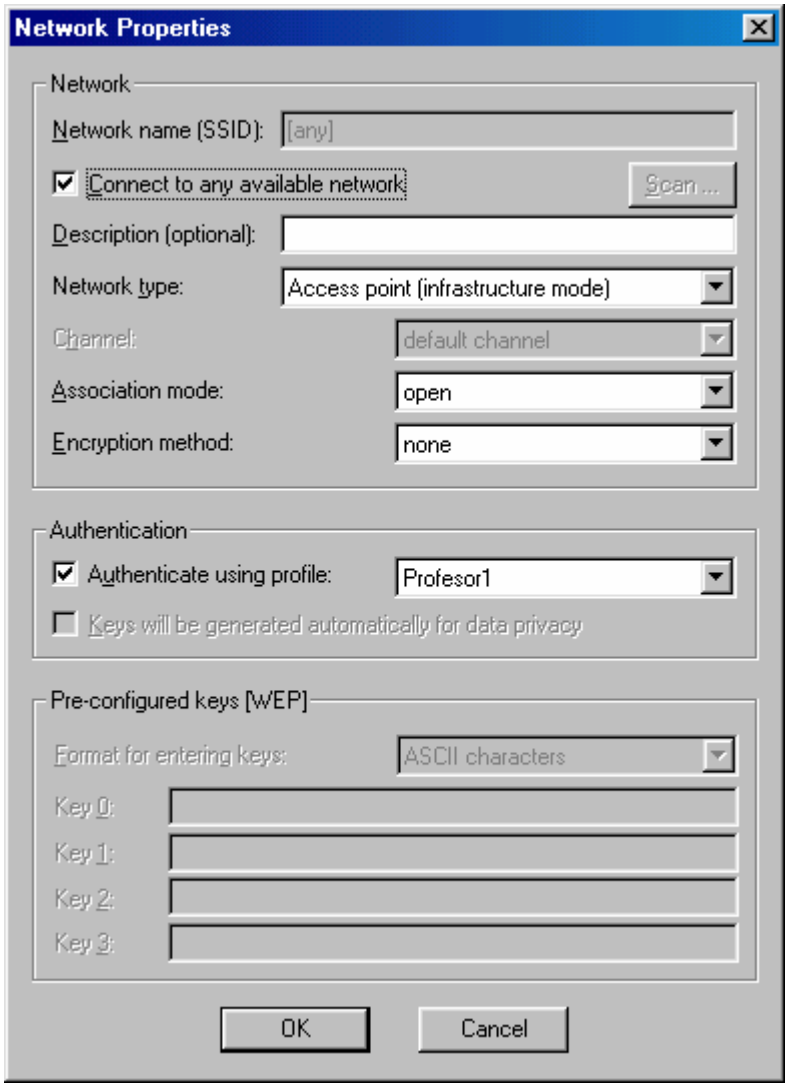

Figura -3.9- Ventana de configuración de las redes relacionadas con el cliente *Odyssey*

autenticar la conexión, para el caso por ejemplo, del usuario profesor1, sería el perfil Profesor1 el elegido en esta opción. Se pulsa *"OK"* y los cambios quedan almacenados.

La última opción que se ha de configurar es la opción *Adapters* donde aparecerán los adaptadores de red, bien cableados o inalámbricos, del equipo donde se está ejecutando el cliente. El programa detecta durante la instalación

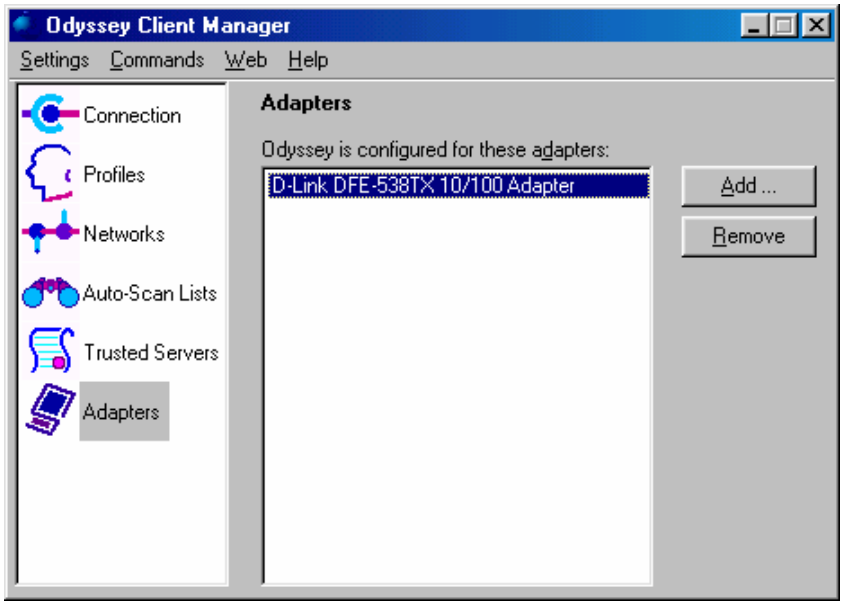

Figura -3.10- Ventana donde se le indican las interfaces sobre las que actuará el cliente Odyssey

todos los adaptadores de red del equipo, aún así en caso de que se quiera añadir un nuevo adaptador o el programa no haya incluido alguno de los adaptadores del equipo en la lista, éstos pueden ser añadidos pulsando el botón *Add*, de manera que se entra en un menú en el que se pueden añadir tanto adaptadores cableados como inalámbricos.

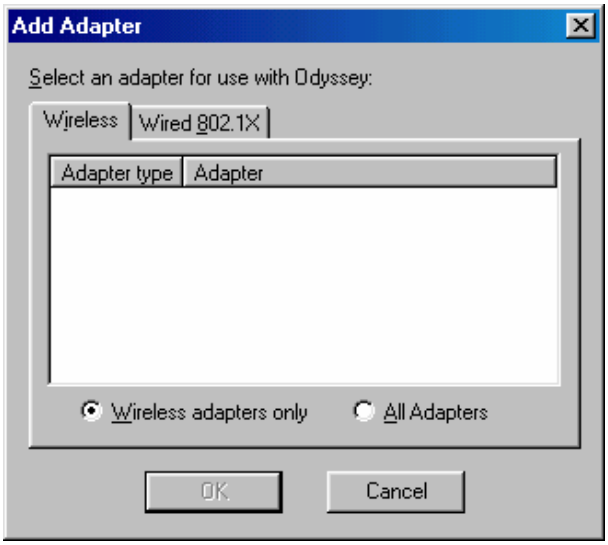

Figura -3.11- Ventana para añadir una nueva interfaz

Dichos adaptadores también pueden eliminarse de la lista de adaptadores mediante el botón *Remove*.

Por último, desde la ventana *Connection* se elige el adaptador de red mediante el cual se va a llevar a cabo la autenticación marcándolo en el menú desplegable *Adapter*, en este caso es un adaptador cableado *D-link DFE-538TX 10/100 Adapter*. Acto seguido se activa la casilla *Connect using profile*, para el ejemplo que se está usando se elige del menú desplegable el perfil *Profesor1*.

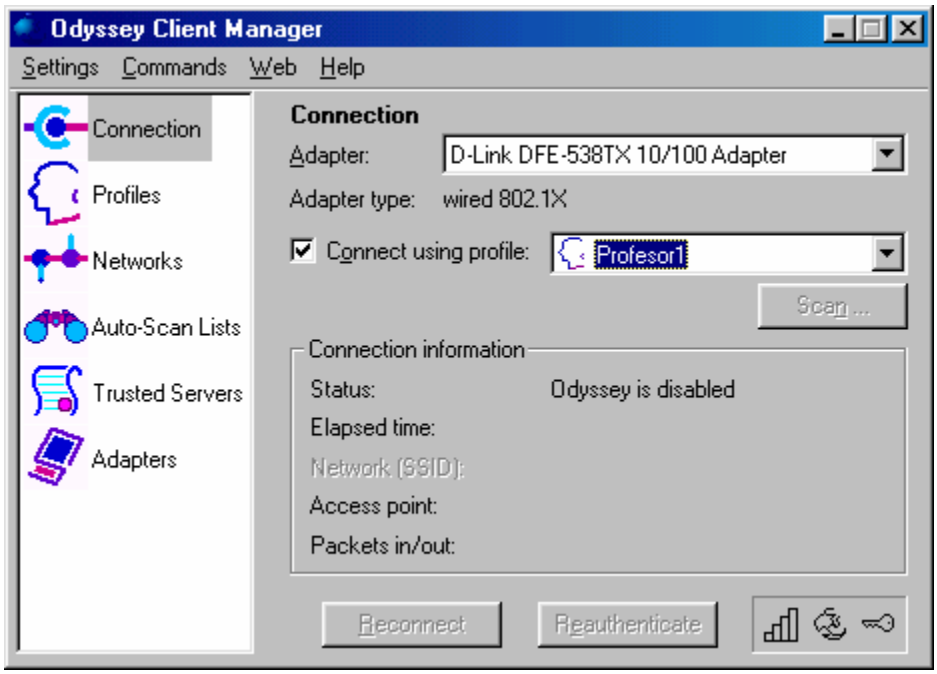

Figura -3.12- Ventana connection del cliente *Odyssey* configurada para realizar la conexión con el perfil de usuario “profesor1”

3.4.4 Puesta en marcha del Business Policy Switch 2000

3.4.4.1 Configuración inicial del BPS 2000

La configuración inicial del BPS consiste en dotar a éste de una dirección IP mediante la cual poder acceder al conmutador posteriormente mediante Telnet o Web. Este último es el escenario desde donde se va a configurar el BSP para la realización del ejercicio propuesto en este capítulo. Para asignarle una dirección IP al BPS 2000 se siguen una serie de pasos. En primer lugar hay que conectar el PC desde donde se desea configurar el conmutador a dicho conmutador mediante un cable cruzado a través del puerto serie. Una vez conectado el cable se abre el programa *Hyperterminal* de *Windows* y se crea una nueva conexión, para ello se arranca el programa *Hyperterminal* y desde el menú *Archivo -> Nueva Conexión* se le asigna un nombre

Figura -3.13- Ventana donde se proporciona de un nombre a la conexión

para la conexión y se pulsa *Aceptar*. A continuación, se asigna la conexión al puerto (COM1 ó COM2) al que se haya conectado el cable cruzado que conecta el PC con el BPS 2000.

Figura -3.14- Ventana de configuración del tipo de conexión que se establece mediante el programa *Hyperterminal*

Una vez elegido el puerto se pulsa Aceptar. Para la conexión se configuran las siguiente priopiedades:

- Bits por segundo: 9600

- Bits de datos: 8
- Paridad: Ninguna
- Bits de parada: 1
- Control de flujo: Xon/Xoff

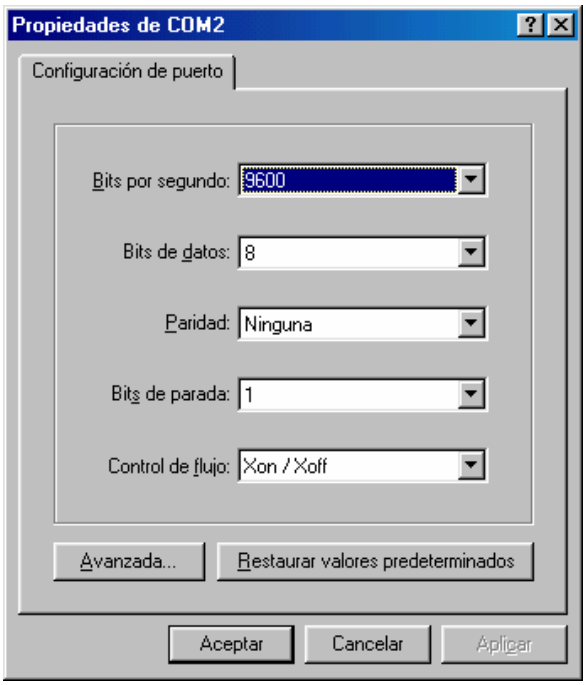

Figura -3.15- Ventana de configuración del puerto

Se pulsa aceptar y ya está configurada y abierta la conexión del *Hyperterminal* para el BPS 2000. Una vez abierta la conexión se arranca el BPS y tras la secuencia de arranque del BPS se observa en la ventana del *Hyperterminal* un menú como el que aparece en la figura:

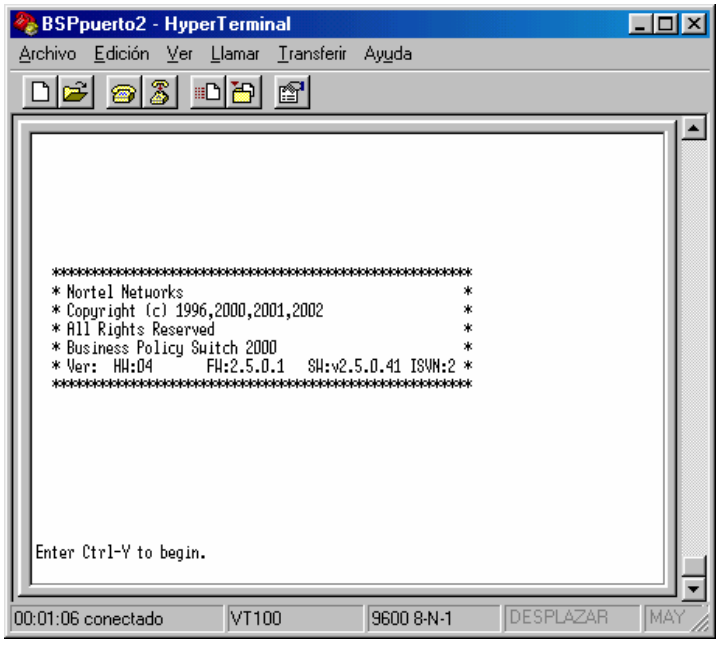

Figura -3.16- Mensaje recibido al conectarse al BSP 2000 mediante *Hyperterminal*

Pulsando *Ctrl.+Y* accedemos a la línea de comando, caracterizada por el siguiente *prompt*.:

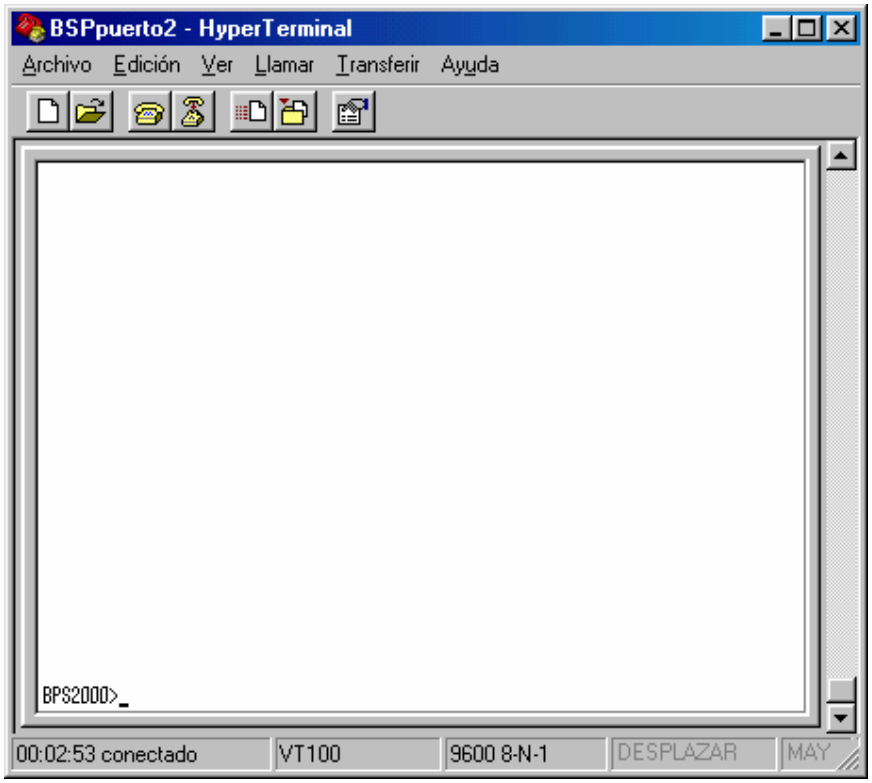

Figura -3.17- Línea de comandos del BPS 2000 en modo *User-EXEC*

La línea de comandos tiene varios modos, para la realización del ejercicio propuesto en este capítulo interesan los tres primeros modos:

- *User-EXEC*: Es el modo por defecto. En este modo el usuario solo dispone de un reducido grupo de comandos a ejecutar.
- *Privileged EXEC*: El usuario tiene a su disposición más comandos que en el modo anterior, que le permiten realizar una configuración básica del BPS.
- *Global Configuration:* Este modo ofrece un mayor número de posibilidades de configuración tales como dirección IP, acceso Telnet, VLAN, etc.

Existe un modo más denominado *Interface Configuration*, dicho modo no va a ser usado en este proyecto.

Desde la línea de comandos se ejecuta el comando *enable* que hace que el usuario entre en modo *Privileged EXEC*. Una vez dentro de este modo se ejecuta el comando *config* o *configure* para pasar al modo *Global Configuration* ,modo desde el que se asigna al conmutador una dirección IP, para ello basta con ejecutar el siguiente comando:

ip address 192.168.1.60 (se introduce la IP que se le desee asignar al BPS)

```
BPS2000>enable
BPS2000#configure
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
BPS2000(config)#ip address 192.168.1.60
```

Figura -3.18- Secuencia de comandos para asignar las dirección IP 192.168.1.60 al BPS 2000

Puede apreciarse como el *prompt* de la consola va cambiado en función del nivel de usuario en el que se esté trabajando.

Una vez que el BPS ya dispone de una dirección IP, puede accederse a él mediante un navegador introduciendo en la barra de direcciones de éste dicha dirección IP. De este modo se accede a la interfaz Web de gestión del conmutador, donde todas las operaciones referentes a la configuración y manejo del conmutador pueden realizarse mediante una específica y sencilla interfaz gráfica.

3.4.4.2 Actualización del *software*

En el ejercicio propuesto en este capítulo va a usarse el protocolo EAPOL en combinación con un servidor RADIUS. La versión de *software* originalmente instalada en el BPS no implementaba el protocolo EAPOL por lo que tuvo que ser reemplazada por una versión posterior, en concreto la versión 2.5. La actualización debe realizarse en dos pasos:

- En primer lugar cambiar la versión 1.0.1 por la versión 1.1.1 (versión que ya ofrece funcionalidades con EAP).
- A continuación reemplazar la versión 1.1.1 por la versión 2.5.

Para realizar dicha actualización del *software* se hace uso de un servidor TFTP (*Trivial File Transfer Protocol*), en este caso va a utilizarse el *software TFTPSuitePro* de *SolarWinds*, *software* que proporciona tanto un cliente como un servidor TFTP aunque en este caso solo va a utilizarse el servidor ya que el cliente está incluido en el Businnes Policy 2000 que será el que actúe como tal. Una vez descargado el *software* desde la página de *SolarWinds* http://solarwinds.net se procede a la instalación del mismo mediante un sencillo *wizard*. Finalizada la instalación puede arrancarse el programa desde el menú *Inicio -> programas -> TFTPSuitePro2000 -> TFTPServer32*. En el apéndice C se ha incluido una descripción breve de las características más significativas de dicho servidor TFTP con la intención de facilitar su uso en este proyecto.

3.4.4.3 Configuración del BPS 2000

Una vez realizada la configuración inicial y la actualización del *software* del BPS 2000, se procede a la configuración del mismo. Para ellos se abre un navegador de Internet y en la barra de direcciones se introduce la dirección IP del BPS 2000, de modo que se accede a la interfaz de configuración y gestión del conmutador. En dicha

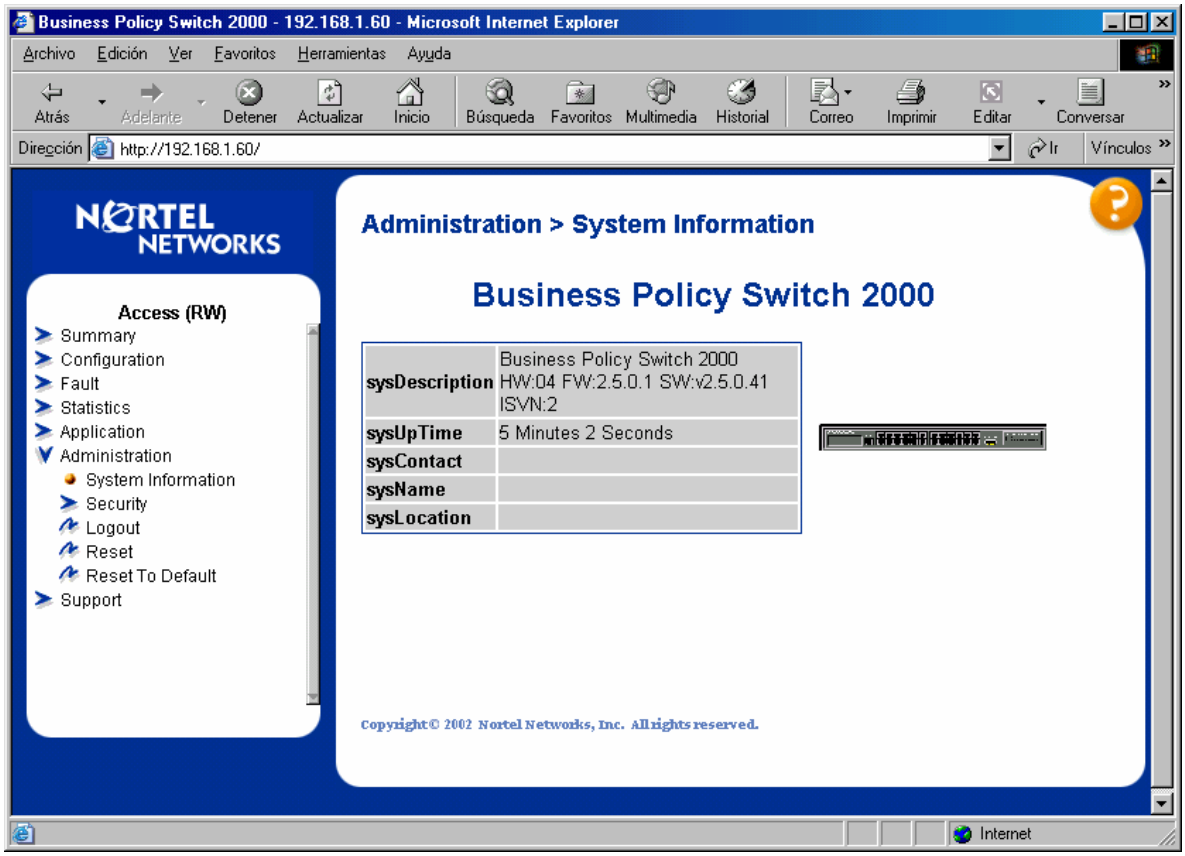

Figura -3.19- Interfaz Web de administración del BPS 2000

interfaz de configuración, pueden gestionarse la totalidad de las funciones del conmutador de una forma fácil y cómoda. A medida que avance este documento se van a ir haciendo hincapié en aquellas partes de la interfaz necesarias para la resolución del ejercicio.

Protección del acceso a la interfaz Web de gestión

El primer paso (en lo que a configuración de la seguridad en el BPS se refiere) va a ser proteger la interfaz Web de administración del conmutador. Para ello se usará autenticación remota mediante un servidor RADIUS, para restringir el acceso a dicha interfaz de gestión.

Para ello, en primer lugar, han de configurarse los parámetros del conmutador referentes al servidor RADIUS para lo que dentro del panel que se observa a la izquierda de la interfaz se entra en el apartado *Administration* (que es el apartado donde aparece el usuario por defecto). Dentro de éste en el apartado *Security*, y a continuación en *RADIUS* donde se encuentran todos los parámetros del conmutador relativos a la configuración del servidor RADIUS. La interfaz de configuración consta de las siguientes partes:

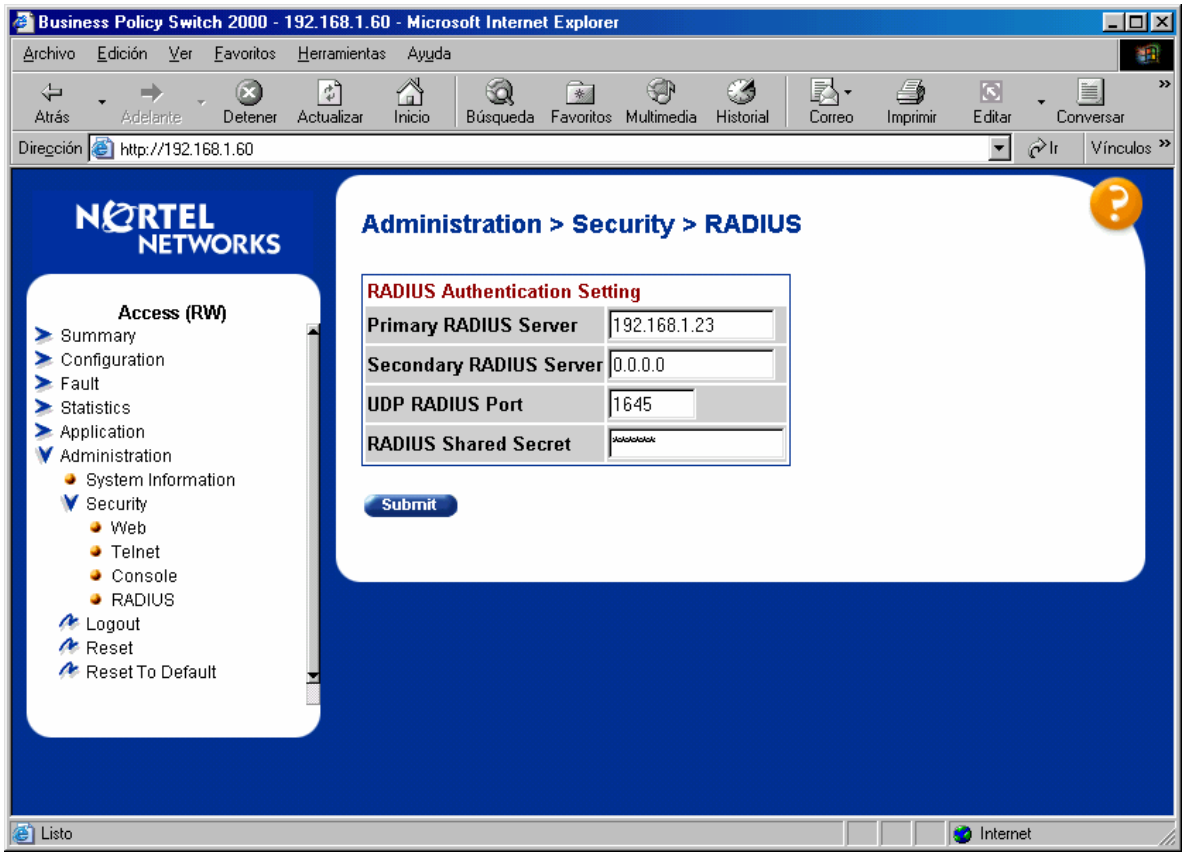

Figura -3.20- Apartado de configuración del servidor RADIUS que se comunicará con el BPS 2000

- *Primary RADIUS Server*: Campo en el que se especifica la dirección IP del servidor RADIUS primario, es decir el primer servidor RADIUS con el que intentará ponerse en contacto.
- *Secondary RADIUS Server*: Dirección IP del servidor RADIUS secundario al que se recurrirá en caso de indisponibilidad o fallo del primario
- *UDP RADIUS Port*: Puerto en el que se ejecuta el servidor RADIUS.
- *RADIUS Shared Secret*: Secreto compartido entre el cliente (en este caso el BPS 2000) y el servidor RADIUS.

Para el ejercicio planteado los valores a rellenar son los siguientes:

- *Primary RADIUS Server*: 192.168.1.23
- *Secondary RADIUS Server*: 0.0.0.0 (no se dispondrá de servidor secundario)
- *UDP RADIUS Port*: 1645
- *RADIUS Shared Secret*: bienve

Una vez rellenados los valores de los campos se pulsa el botón *Submit* y los cambios se actualizan al instante.

Una vez configurados los parámetros del conmutador relacionados con el servidor RADIUS queda indicarle al conmutador que proteja el acceso a la interfaz Web haciendo

uso de dicho servidor RADIUS. Para ello dentro del apartado *Administration -> Security* se entra en el apartado *Web* desde donde podemos restringir los futuros accesos Web al conmutador mediante una clave. Se abre el menú desplegable y se observan tres opciones:

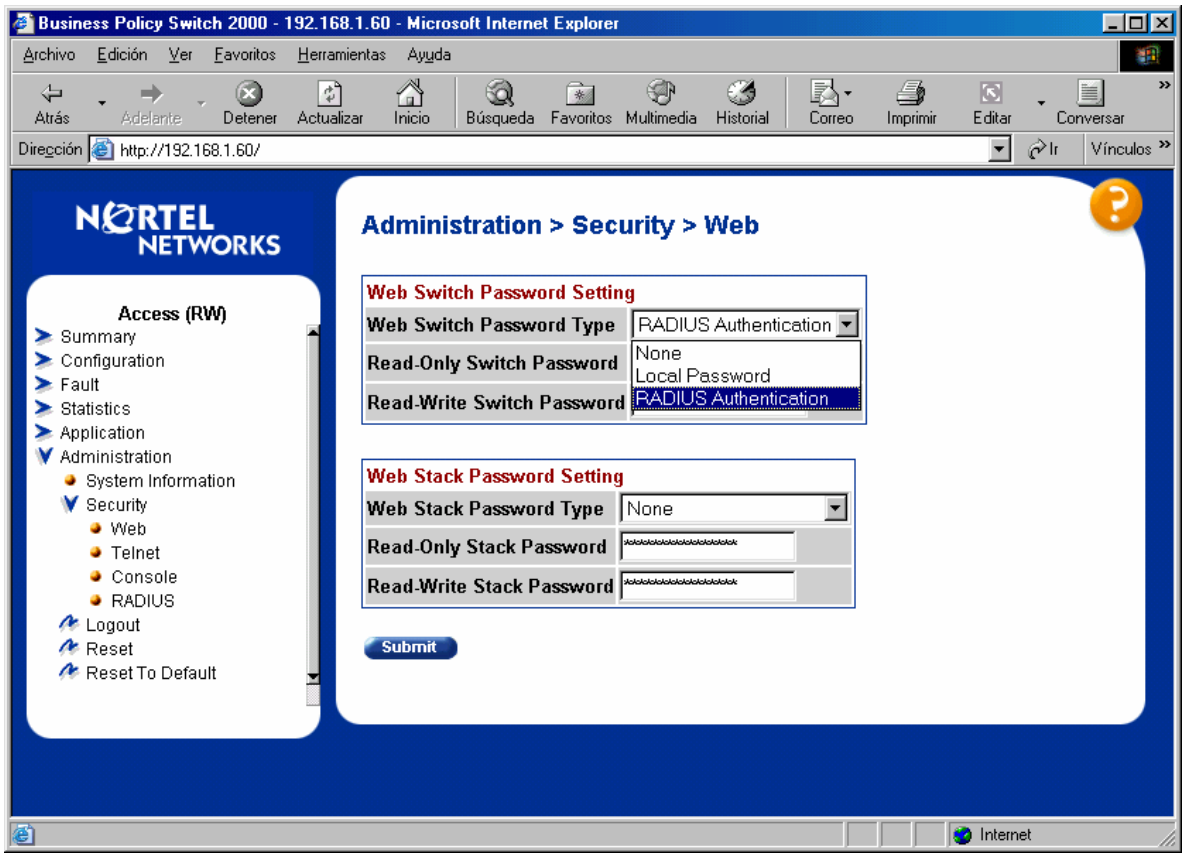

Figura -3.21- Interfaz Web de configuración del control de acceso al BPS 2000

- *None*: Permite el acceso libre a la interfaz Web de configuración.
- *Local*: Exige un clave local para acceder a la interfaz Web.
- *RADIUS Authentication*: El acceso Web está protegido mediante identificador de usuario y una claveverificados por un servidor remoto de autenticación usando el protocolo RADIUS.

De las tres opciones, se elige la opción *RADIUS Authentication* y se pulsa el botón *Submit* para actualizar los cambios. Para asegurarse de esto último se recomienda reiniciar el BPS 2000 lo cual puede llevarse a cabo de una forma sencilla mediante el apartado *Reset* situado en la interfaz Web de gestión.

A partir de este momento cada vez que se intente acceder al conmutador a través del navegador mediante su dirección IP aparecerá una interfaz de *login* de la siguiente forma:

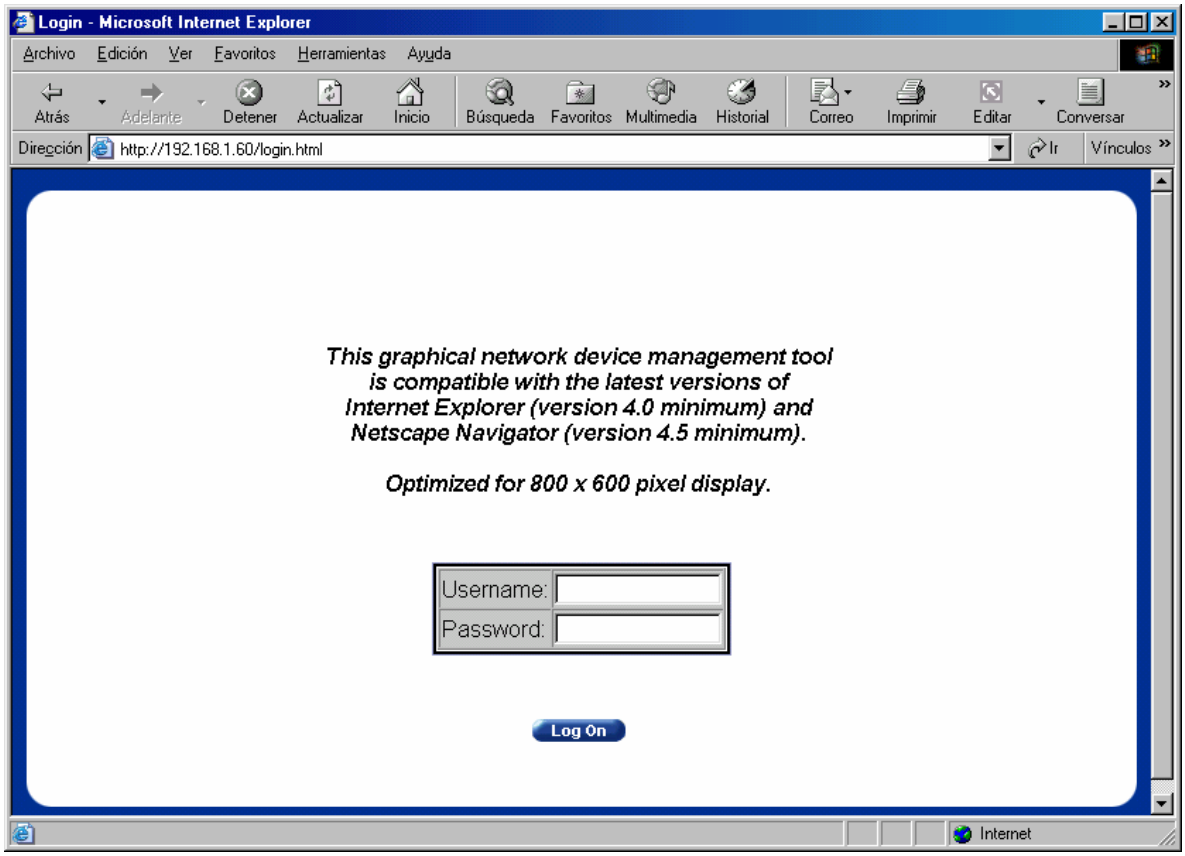

Figura -3.22- Interfaz de *login* para el acceso a la interfaz de gestión del BPS 2000

Previamente se ha configurado en el servidor RADIUS una entrada en el fichero de configuración ***users*** con el identificador de usuario *adminSys*, para el cual se ha especificado el uso de autenticación mediante el protocolo EAP, concediéndole al usuario, siempre y cuando el resultado de la autenticación sea positivo, permisos de administración del sistema.

Por lo tanto, se introduce el identificador de usuario y la clave correspondiente, previamente configurados en el fichero ***users*** del servidor RADIUS:

Login: *adminSys*

Clave: *passadminSys*

Una vez introducidos estos valores se pulsa el botón *Log On* accediendo de este modo a la interfaz Web de gestión del conmutador.

Creación de las VLAN

El siguiente paso que va a llevarse a cabo es la creación de las VLAN. Para ello dentro de la interfaz Web de gestión hay que dirigirse al apartado *Application -> VLAN-> VLANConfiguration*. Desde aquí pueden configurarse la mayoría de parámetros del

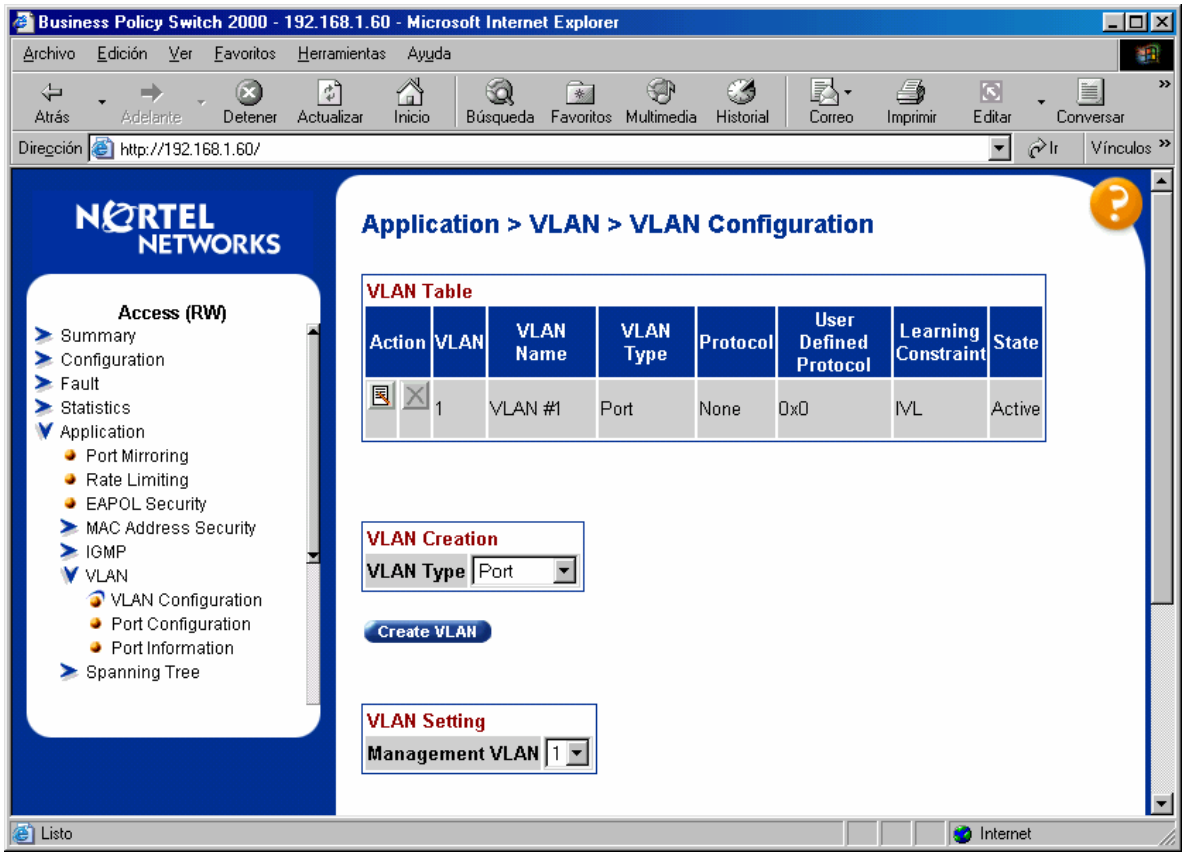

Figura -3.23- Interfaz Web de configuración de VLAN

BPS 2000 asociados a las VLAN, Puede observarse una tabla en la que aparecen todas la VLAN creadas en el BPS 2000 así como las características más relevantes de las mismas.

Las opciones de configuración para VLAN que proporciona esta interfaz son las siguientes:

- ***VLAN Creation***: El BPS 2000 permite crear tres tipos de VLAN:
  - *Port*: basadas en puertos.
  - *Protocol*: basadas en protocolo
  - *MAC SA*: Basadas en la dirección MAC de la fuente

Para saber más acerca de estos tres tipos de VLAN puede dirigirse al apartado 3.1.2.

Pulsando el botón *Create VLAN* accede a la ventana de creación de VLAN del tipo elegido. En este caso el tipo de VLAN va a ser port-based, ya que es el tipo de VLAN que permite trabajar con “Automatic PVID”. La ventana de configuración presenta las siguientes características:

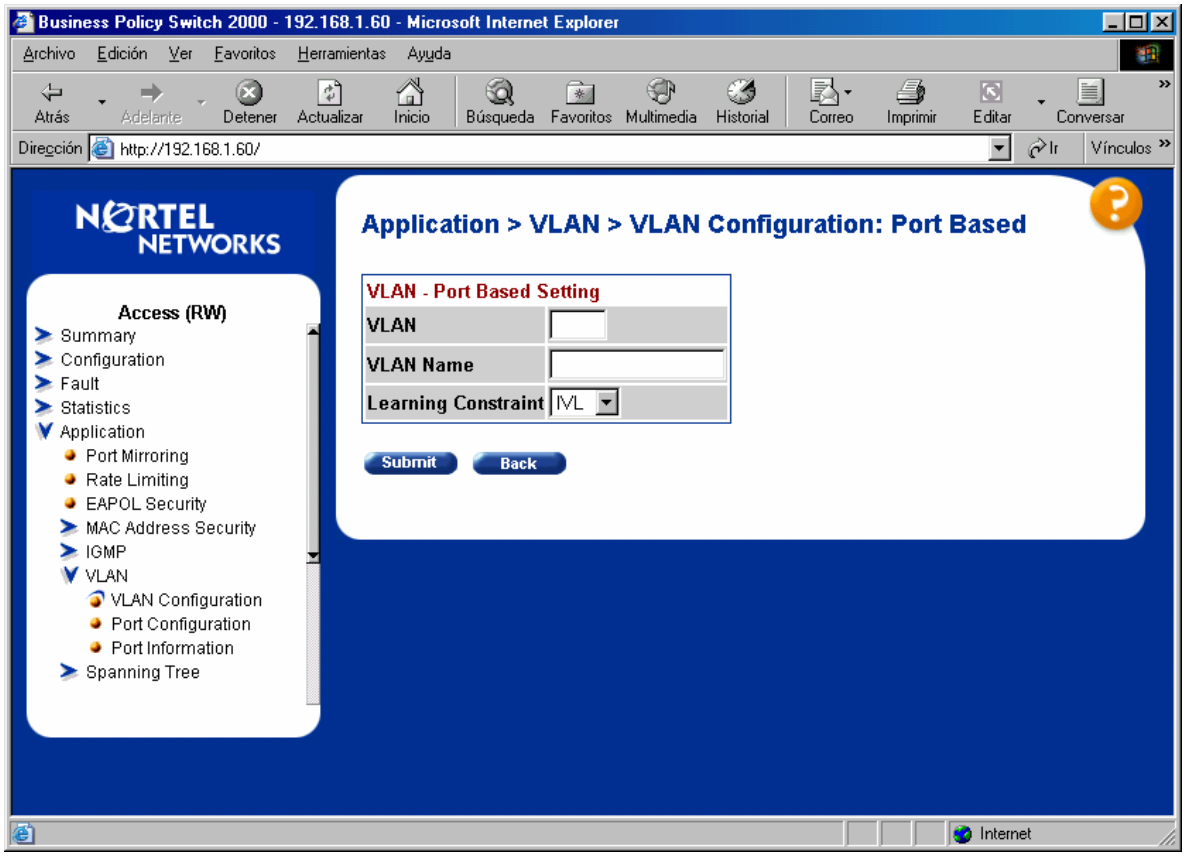

Figura -3.24- Interfaz de configuración de una VLAN basada en puertos

- *VLAN*: Consiste en el numero asignado a la VLANque va a crearse.
- *VLAN Name*: Nombre con el que se identifica la VLAN.
- *Learning Constraint*: en este apartado se especifica si la VLAN compartirá su base de datos de filtros con otras o tendrá la suya propia. Para el ejercicio se deja la configuración que aparece por defecto, IVL, es decir, una base de datos propia de cada VLAN.

Para el ejemplo de la VLAN2, se introducen los siguientes datos:

- VLAN: 2.
- VLANName: VLANInvitados.
- Learning Constraint: IVL.

Se pulsa el botón *Submit* y la VLAN queda añadida a la tabla de VLAN tal y como puede apreciarse en la figura:

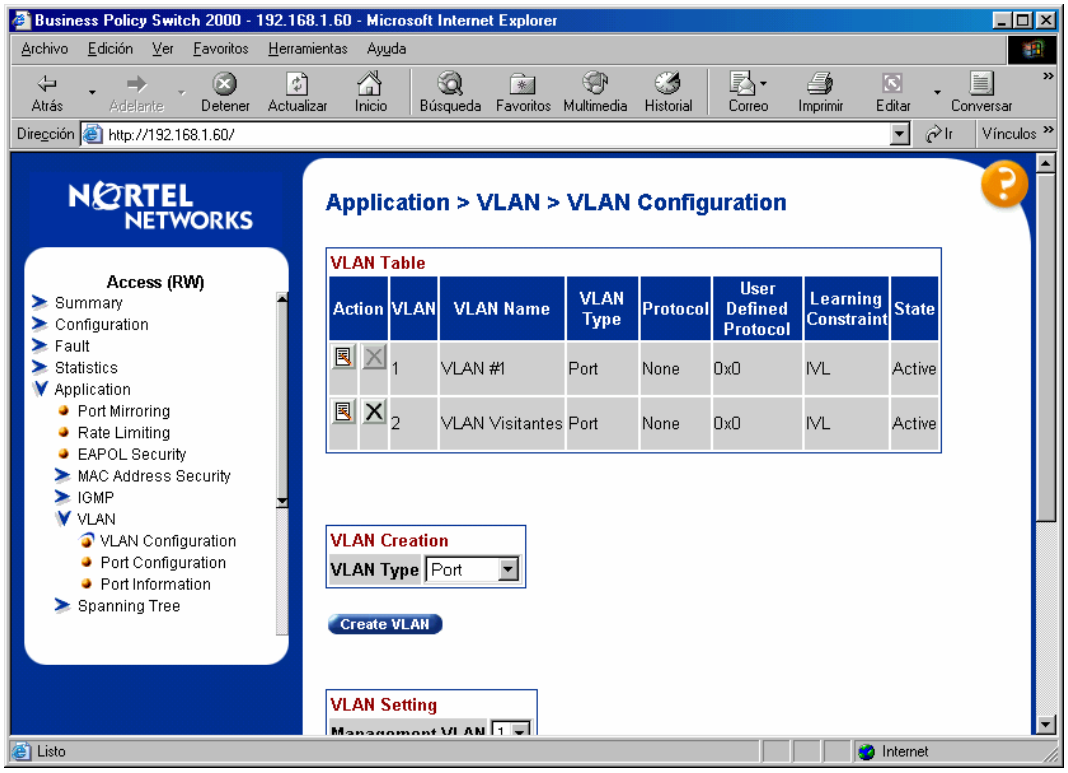

Figura -3.25- Interfaz Web con la lista de VLAN creadas

Para crear el resto de VLAN del ejercicio se sigue el mismo procedimiento. Una vez creadas todas las VLAN, quedan por configurar el resto de parámetros disponibles en la interfaz.

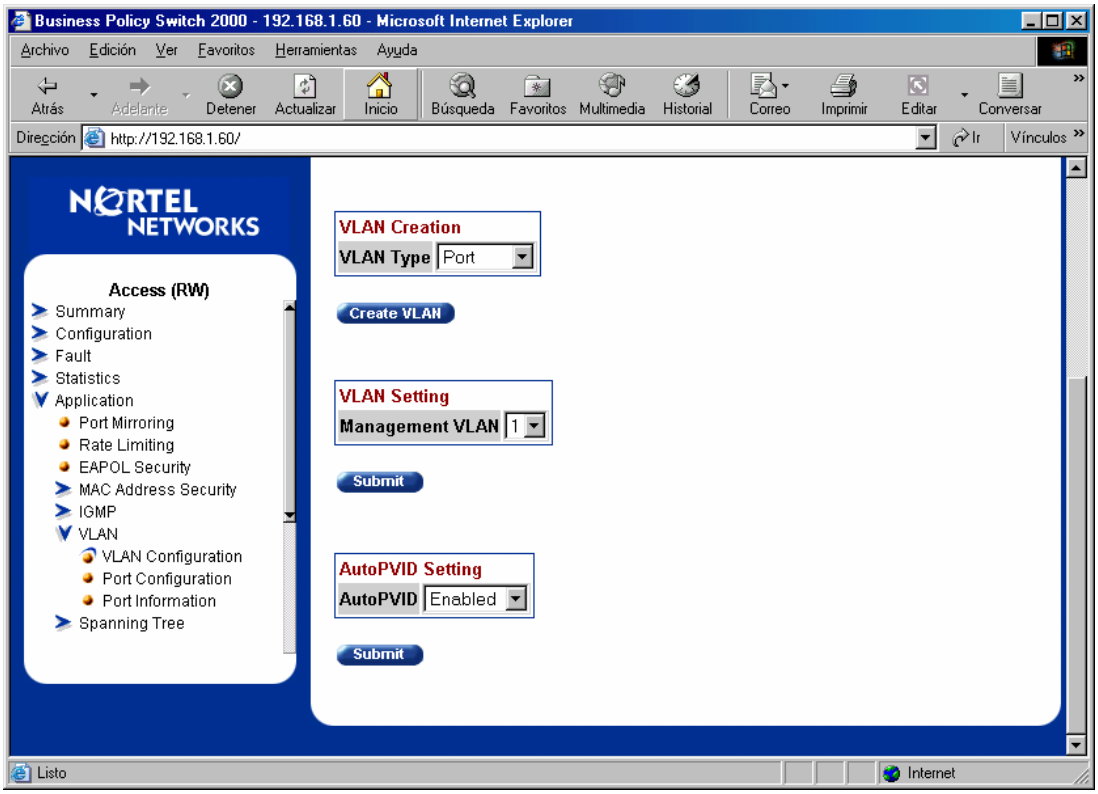

Figura -3.26- Opciones ofrecidas por la interfaz Web para la creación de VLAN

- VLANSetting:
  - Management VLAN: En este campo se elige la VLAN desde la que se permitirá administrar el conmutador. Para el ejercicio se dejará la opción por defecto, es decir, la VLAN1 será aquella desde la que se puede administrar y configurar el conmutador, para lo que se marca un "1" en el menú desplegable y se pulsa el botón *Submit*.
- AutoPVID Setting:
  - AutoPVID: Se escoge la opción *Enabled* para activar esta característica en el conmutador. De modo que se permita el cambio automático del parámetro PVID (parámetro que relaciona a un puerto con una determinada VLAN).

Una vez creadas las VLAN pueden editarse o eliminarse, haciendo uso de los botones que aparecen junto a las mismas en la tabla de VLAN. Pulsando el botón  se accede a las opciones de configuración referentes a la VLAN en cuestión. De dichas opciones se ofrece la posibilidad de modificar dos: el nombre de la VLAN y los puertos que son asignados a la misma en la opción *Port Membership*. Un mismo puerto puede aparecer como miembro de varias VLAN.

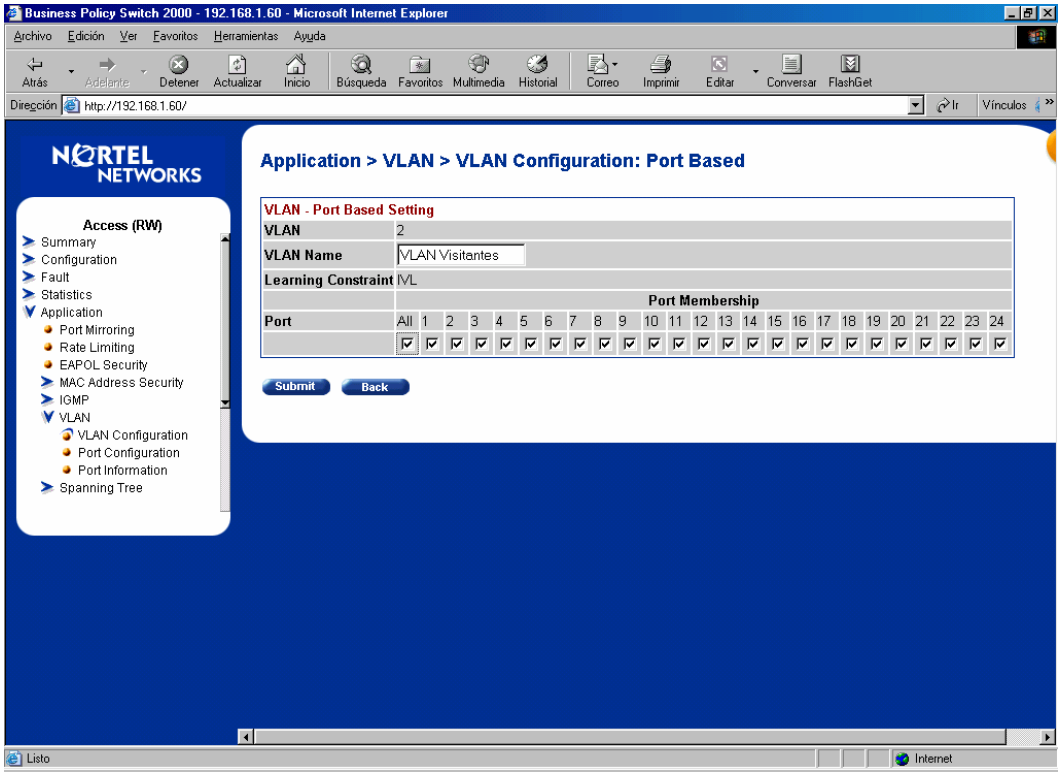

Figura -3.27- Interfaz de configuración de los puertos que serán miembros de una determinada VLAN

El siguiente paso es configurar los puertos, parte indispensable ya que en ellos se basan las VLAN creadas. Para ello dentro del menú *Application -> VLAN-> Port Configuration* se fija para todos los puertos el valor del PVID a 1, de este modo se

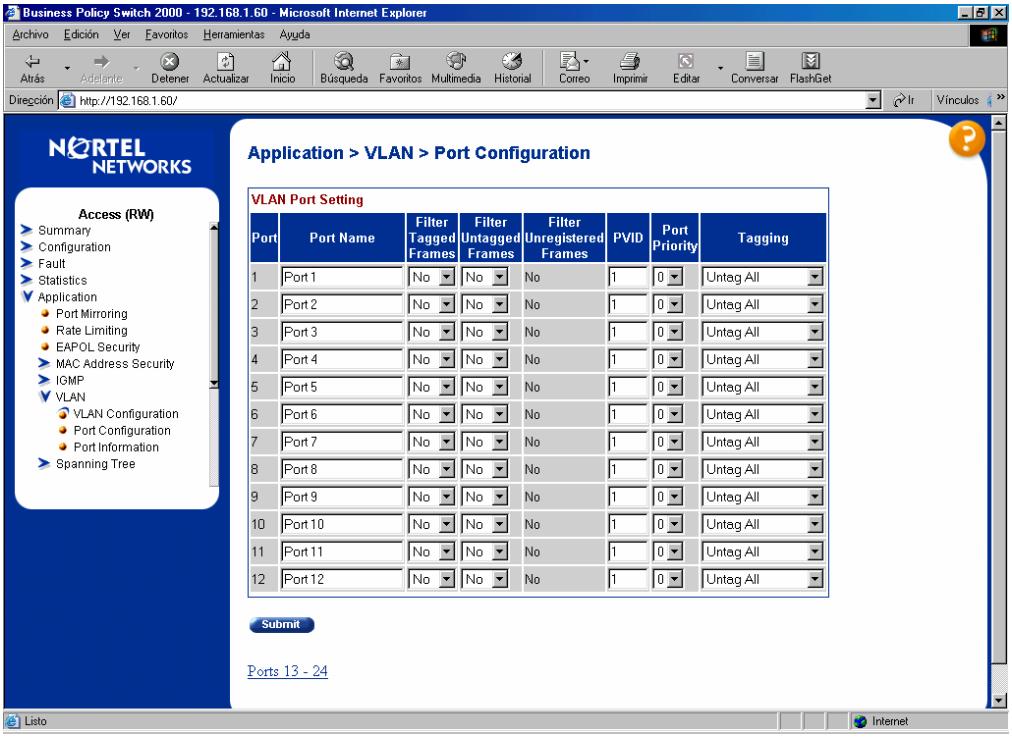

Figura -3.28- Interfaz de configuración de los puertos del BPS 2000

asocian todos los puertos a la VLAN1, que cabe recordar que es la *management VLAN*. A continuación, se pulsa el botón *Submit* para actualizar los cambios.

Seguridad EAP

La siguiente opción a configurar es la referente al uso del protocolo de autenticación EAP. Para ello dentro de *Application* > *EAPOL Security* se configuran

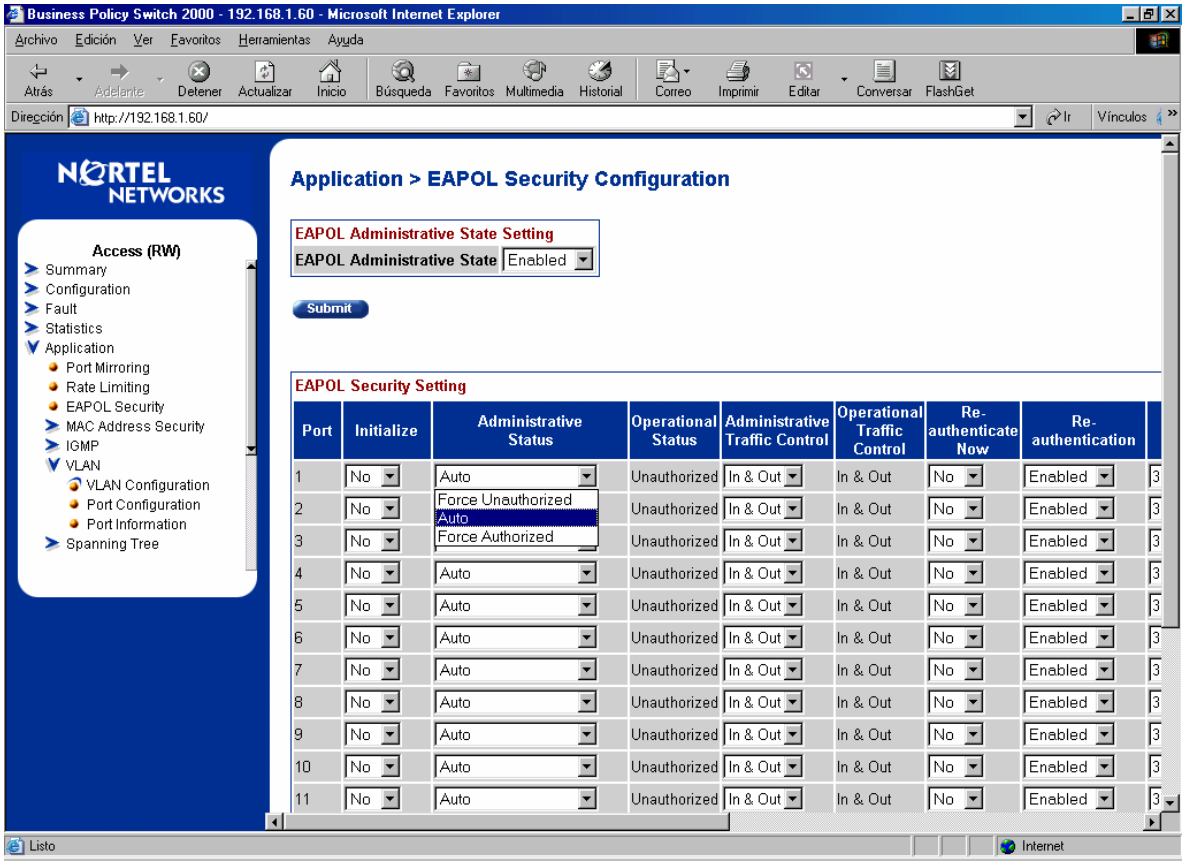

Figura -3.29- Interfaz de configuración de la seguridad EAPOL

los parámetros correspondientes. En primer lugar para cada puerto, excepto para el puerto al que se conecta el servidor RADIUS, en la opción *Administrative Status* se marca la opción *Auto*, de este modo el estado del puerto depende del resultado de la autenticación EAP. Una vez hecho esto en la opción *EAPOL Administrative State* se marca *Enabled* para activar la seguridad mediante protocolo EAPOL en el conmutador.

3.4.5 Autenticación

Una vez configurados todos los parámetros descritos anteriormente, el funcionamiento del sistema sería el siguiente:

Se activa el cliente Odyssey desde el menú de ventana *Settings -> Enable Odyssey*. El cliente nos muestra en pantalla entonces una ventana donde introducir un clave para el usuario elegido, se teclea la clave correspondiente y se pulsa el botón

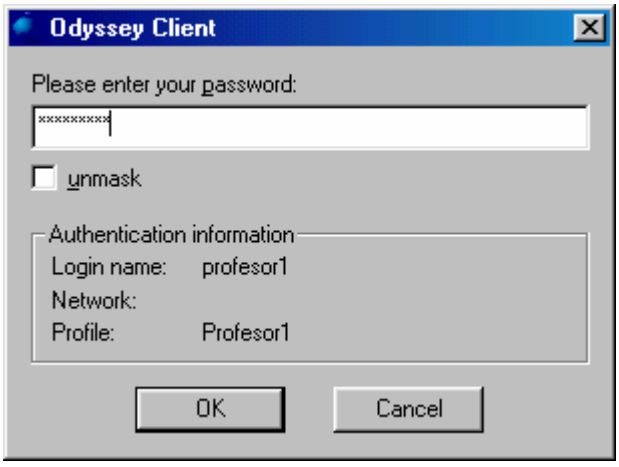

Figura -3.30- Cuadro de diálogo donde el usuario introduce la calve para su autenticación

"OK", si no ha habido ningún error el programa abrirá y autenticará la conexión haciendo eco de ello en el panel *Connection information* mediante el mensaje *Open and Authenticated* en el campo *Status*.

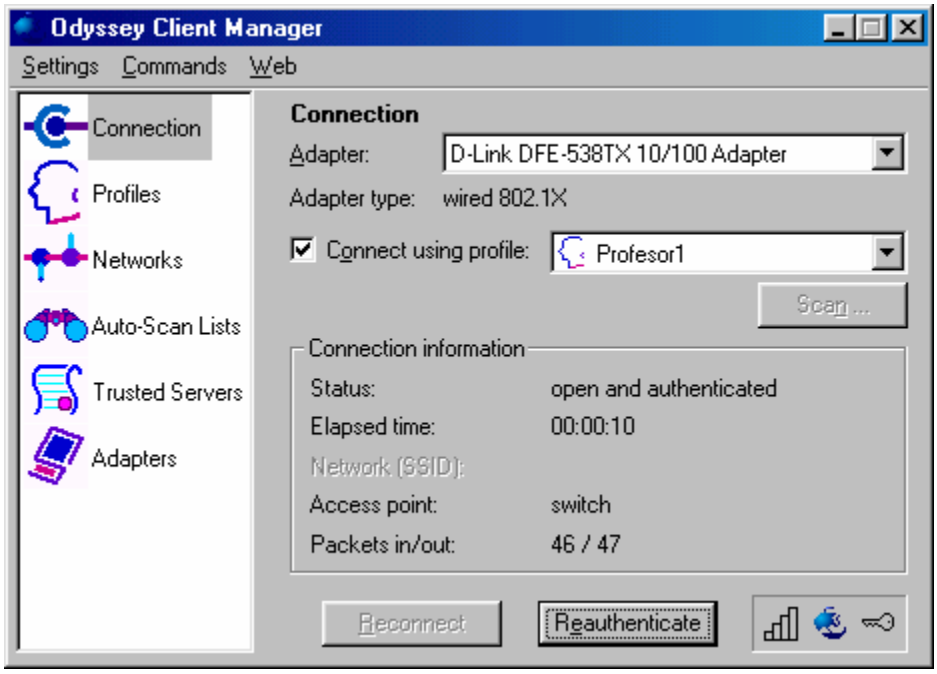

Figura -3.31- Ventana Connection del cliente Odyssey tras una autenticación con resultado positivo

El procedimiento a seguir para autenticar cualquier otro usuario configurado en el servidor RADIUS del mismo modo a los aquí descritos sería idéntico al explicado para el usuario *profesor1*.

La autenticación del usuario consta de dos pasos, los cuales quedan reflejados en los esquemas 1 y 2:

- A cualquier usuario que se conecte a uno de los puertos del BPS 200 desde cualquier máquina le será reclamada (a través del cliente EAP *Odyssey* configurado correctamente) una clave para autenticarse, siguiendo el proceso que se muestra en la figura 3.32.
- Una vez que el servidor RADIUS haya comprobado sus credenciales de usuario en el fichero ***users*** almacenado en el propio servidor RADIUS, devolverá una respuesta al usuario, tal y como se muestra en la figura 3.33, autenticando la conexión o rechazando la misma, además encuadrará al usuario en su VLAN correspondiente mediante los parámetros almacenados en el servidor de autenticación para el usuario en cuestión.

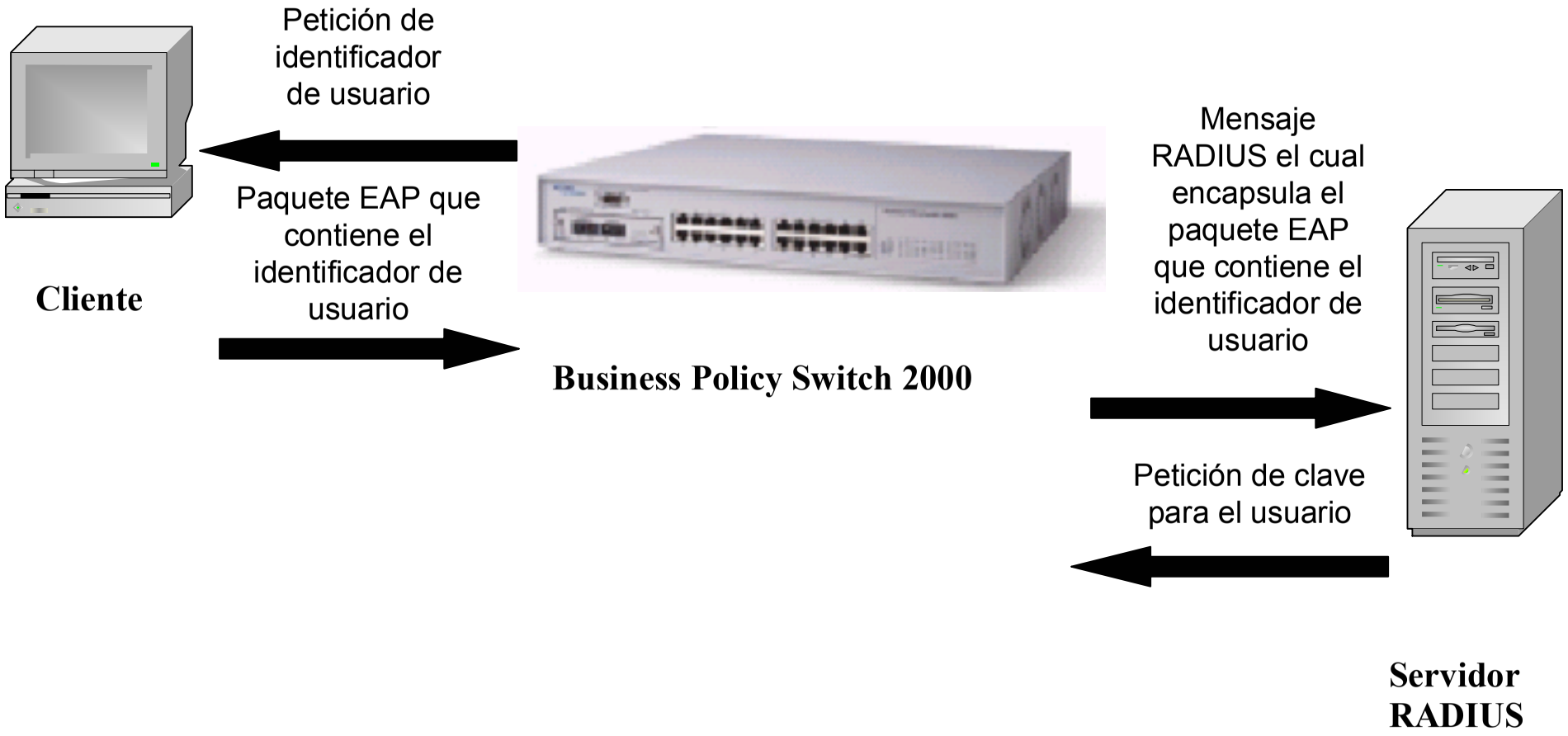

Figura -3.32- Autenticación: Paso 1

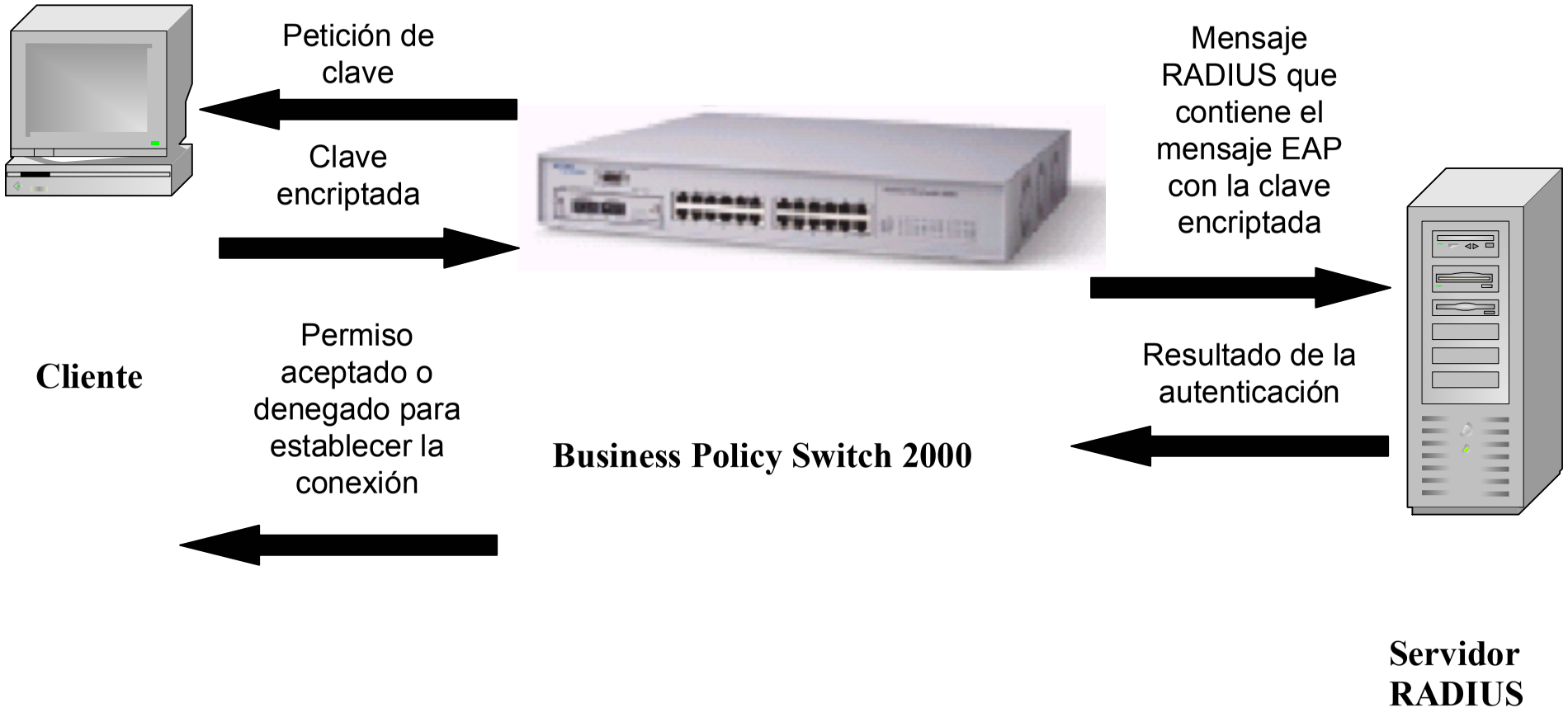

Figura -3.33- Autenticación: Paso 2

Capítulo 4
Conclusiones

Una vez concluida la realización del proyecto, se exponen en este capítulo las conclusiones obtenidas a partir de los resultados alcanzados.

En cuanto a los dispositivos usados en el desarrollo de este proyecto cabe destacar que tanto Business Policy Switch 2000 como Contivity 400 son dos dispositivos muy adecuados para su uso como herramientas docentes ya que ambos ofrecen una interfaz gráfica de configuración que destaca por su sencillez y a su vez por su alta funcionalidad. De este modo, un usuario con unos conocimientos básicos que se disponga a trabajar con cualquiera de ellas, puede obtener un alto rendimiento realizando operaciones de funcionalidad compleja pero fácil configuración. Claros ejemplos de este hecho son los dos ejercicios resueltos en este proyecto, en los cuales mediante una configuración relativamente sencilla se han resuelto problemas complejos de filtrado en uno y de control de acceso del personal de una universidad a distintos grupos de trabajo, en otro.

Una de las herramientas fundamentales con las que se ha trabajo en este proyecto es el cortafuegos. Los beneficios de usar un cortafuegos con respecto a no usarlo son evidentes. Pero en este proyecto, además, se ha usado un cortafuegos dentro de una arquitectura DMZ. Este tipo de arquitectura elimina multitud de problemas de seguridad, dado que al aislar las máquinas más vulnerables de la red (en este caso el servidor Web y el servidor de Correo, es decir, servidores que se pretende que sean de acceso público) del resto de máquinas de la red interna se evita que si un intruso accede a alguna de dichas máquinas especialmente vulnerables, pueda acceder también a las demás. De este modo se aumenta la protección de la red interna, obligando a los posibles intrusos a sobrepasar otra barrera de seguridad adicional que separa a los servidores de acceso público de la red interna. Hay dos variantes de la arquitectura DMZ, en este proyecto se ha optado por la opción de usar un único cortafuegos con varias interfaces de red. Esta opción tiene sus ventajas con respecto a la otra opción, que es la de usar varios cortafuegos con una única interfaz de red. La primera opción minimiza el coste y centraliza la resolución del problema, cumpliendo además con los mismos requisitos de seguridad que la segunda opción ya que cada interfaz actuaría como un cortafuegos de una sola interfaz, con su propio filtro de entrada y su propio filtro de salida.

Para la resolución del problema de seguridad planteado en el capítulo 3 se ha optado por utilizar la tecnología VLAN. Esta decisión se ha tomado previo estudio de las características y servicios que proporcionaba la tecnología VLAN, así como de sus numerosas ventajas respecto a otras opciones. El hecho de usar VLAN para distribuir al personal de la universidad en distintos grupos de trabajo tiene numerosas ventajas:

- Movilidad: El uso de VLAN permite la total movilidad física de los usuarios dentro de los grupos de trabajo. Los grupos de trabajo están construidos como dominios lógicos, independientemente de las conexiones físicas.
- Control y conservación del ancho de banda: el uso de VLAN restringe los *broadcast* a los dominios lógicos donde se han generado, con el consiguiente ahorro de ancho de banda. Además, añadir usuarios a una

determinada VLAN no afecta ni al ancho de banda de dicha VLAN ni al ancho de banda del resto de grupos de trabajo.

- Conectividad y expansión geográfica: Interconectando varios conmutadores las VLAN pueden expandirse a través de ellos, incluso aunque estén situadas en lugares geográficos distintos.
- Seguridad: Los accesos a las distintas VLAN pueden ser restringidos (por ejemplo, mediante un servidor de autenticación remoto como RADIUS) según las necesidades específicas de cada red, proporcionando un alto grado de seguridad.
- Economía: El uso de la tecnología VLAN no supone ningún coste adicional al de los conmutadores ni tampoco modificación alguna de la estructura de red o cableado. Al contrario, minimiza su uso por lo que reduce los gastos.

Además de la tecnología VLAN se ha hecho uso también de la seguridad basada en el protocolo EAPOL trabajando éste último conjuntamente con un servidor de autenticación basado en el protocolo de seguridad RADIUS.

El uso del protocolo EAPOL ha permitido utilizar la función de asignación dinámica de VLAN que proporciona el mismo. Esta característica, de reciente aparición, aumenta de manera considerable tanto la flexibilidad como la movilidad de la red, permitiendo que cualquier usuario desde cualquier punto de la red pueda conectarse a la misma previa autenticación. Según los parámetros de dicha autenticación el usuario será encuadrado en la VLAN que le corresponda (accediendo sólo a los servicios asignados a dicha VLAN), sin necesidad de estar físicamente conectado a un puerto concreto del conmutador que crea las VLAN (BPS 2000).

En cuanto al servidor RADIUS, en este proyecto se ha optado por usar el servidor de autenticación *FreeRADIUS*. El uso del servidor remoto de autenticación *FreeRADIUS* ha ofrecido una serie de ventajas que ha hecho deseable su uso en detrimento de otras opciones:

- El *software FreeRADIUS* es un *software* de libre distribución por lo que el apartado económico se ve mejorado considerablemente. Simplemente teniendo acceso a Internet el usuario puede hacerse con las fuentes del programa de forma totalmente gratuita.
- *FreeRADIUS* destaca también por su sencillez de instalación y configuración, ésta última se realiza a través de unos *scripts* de configuración que pueden ser modificados a gusto del usuario para cumplir unos requisitos determinados con relativa facilidad.
- Al tener un servidor de autenticación remota RADIUS la seguridad de la red está totalmente centralizada, con lo que se evitan los problemas de dispersión y comunicación de un sistema distribuido.
- La autenticación de los usuarios es totalmente flexible, permitiendo una amplia movilidad de los mismos, ya que sus datos referentes a la autenticación están centralizados en el servidor de autenticación y no en la máquina desde donde se desea conectar el usuario.
- El protocolo RADIUS está siendo extensamente desarrollado y utilizado para añadir seguridad en las comunicaciones actuales, lo que repercute en una gran cantidad de documentación disponible para conocer su funcionamiento. Concretamente, el *software FreeRADIUS* dispone de una amplia gama de referencias donde se especifica tanto su instalación como su posterior configuración. El hecho de que dicho *software* sea un *software* de libre distribución ha influido positivamente en este hecho.

El objetivo fundamental del proyecto ha sido el estudio de la seguridad en redes de comunicaciones, por lo que su realización ha permitido el aprendizaje de múltiples arquitecturas de seguridad así como sus diferentes ventajas e inconvenientes. Asimismo el desarrollo del proyecto ha exigido el estudio de diferentes protocolos y tipos de seguridad como por ejemplo, VLAN, EAP, RADIUS, alguno de ellos de reciente aparición y de uso muy extendido en la actualidad, lo que ha reforzado fuertemente los conocimientos del autor en lo que a estas materias se refiere. Esto ha sido debido a que los problemas planteados por el proyecto son problemas muy extendidos en la actualidad, a los que se dedican múltiples proyectos con la intención de encontrar la solución más efectiva.

Por lo tanto se puede concluir que este proyecto ha sido sobre todo un proyecto con carácter práctico en el que, se han llevado a cabo ejercicios de gran interés, en la actualidad, dado la extensa lista de elementos de seguridad tales como, protocolos, herramientas hardware y *software* utilizados.

Apéndice A
Comprobación del servidor RADIUS

Una vez terminado el proceso de instalación es conveniente comprobar que todo funciona correctamente. Para llevar a cabo dicha comprobación se usará un *software* de libre distribución denominado NTRadPing disponible en http://www.dialways.com. En este caso se va a usar dicha herramienta bajo el sistema operativo *Windows*, una vez se descarga la versión del *software* correspondiente se descomprime el fichero en la ubicación deseada. El paquete está formado por dos ficheros, *raddict.dat* y *NTRadPing.exe*, ejecutando este último se inicia el programa que permite enviar un *ping* al servidor RADIUS. La respuesta del servidor (o la no respuesta en su caso) permite verificar el correcto funcionamiento del servidor. En la figura 1 se muestra la interfaz gráfica del programa:

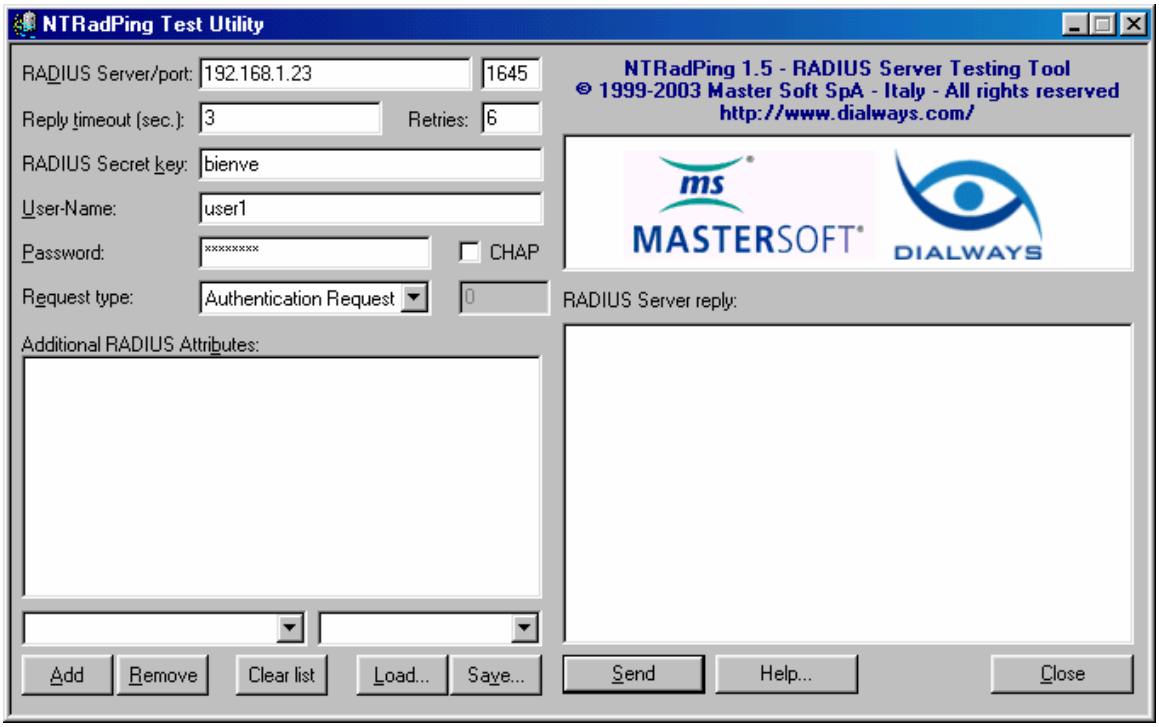

Figura –A.1- Interfaz de la aplicación *NTRadPing Test Utility*

A continuación se describe la funcionalidad de los apartados de esta interfaz gráfica que van a ser de utilidad para la realización del ejercicio planteado:

- ***RADIUS Server/port***: En este campo se especifica la dirección IP de la máquina en la que se está ejecutando el servidor RADIUS así como el puerto en el cual está ejecutándose dicho servidor.

- ***RADIUS Secret Key***: En esta casilla se especifica el secreto que intercambian cliente y servidor. El secreto especificado debe coincidir con el secreto especificado en el fichero de configuración *clients.conf* para la máquina cliente en la que se está ejecutando *NTRadPing*.
- ***User-Name***: Identificador de usuario con el que se desea realizar el *ping* al servidor RADIUS.
- ***Clave***: Aquí se especifica la clave correspondiente al usuario anteriormente indicado en la casilla *User-Name*.
- ***Request-Type***: Indica el tipo de consulta o llamada que se va a realizar al servidor RADIUS.

En nuestro caso, para probar el servidor le asignaremos los siguientes valores a los campos indicados anteriormente:

RADIUS Server/port: 192.168.1.23/1645

RADIUS Secret Key : bienve

User-Name: root

Clave: Nortel

Request-Type:Authentication-Request

El resto de campos se dejan como aparecen por defecto al ejecutar el programa.

Una vez configurados los valores para cada uno de los campos, se pulsa el botón *Send* para enviar la petición, si todo funciona correctamente el servidor RADIUS nos responderá con un *Access-Accept* tal y como se muestra en la figura 2 :

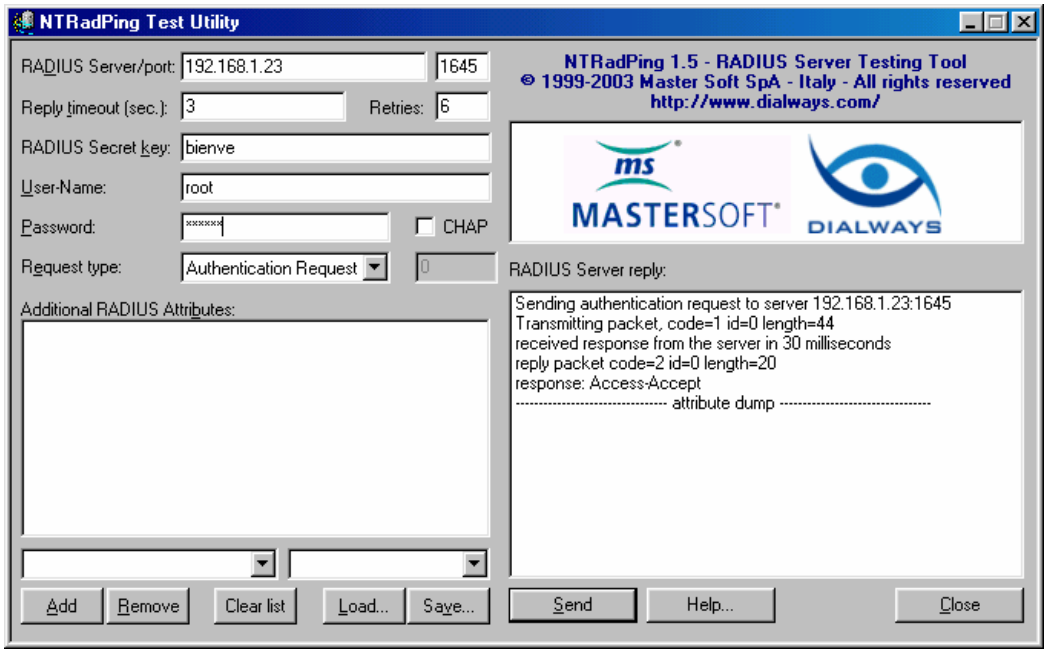

Figura –A.2- *Ping* realizado con éxito

Si se produce algún error (por ejemplo, porque se haya tecleado un nombre de usuario incorrecto), el servidor RADIUS nos responderá con un Access-Reject (Acceso Denegado) tal y como se muestra en la figura 3:

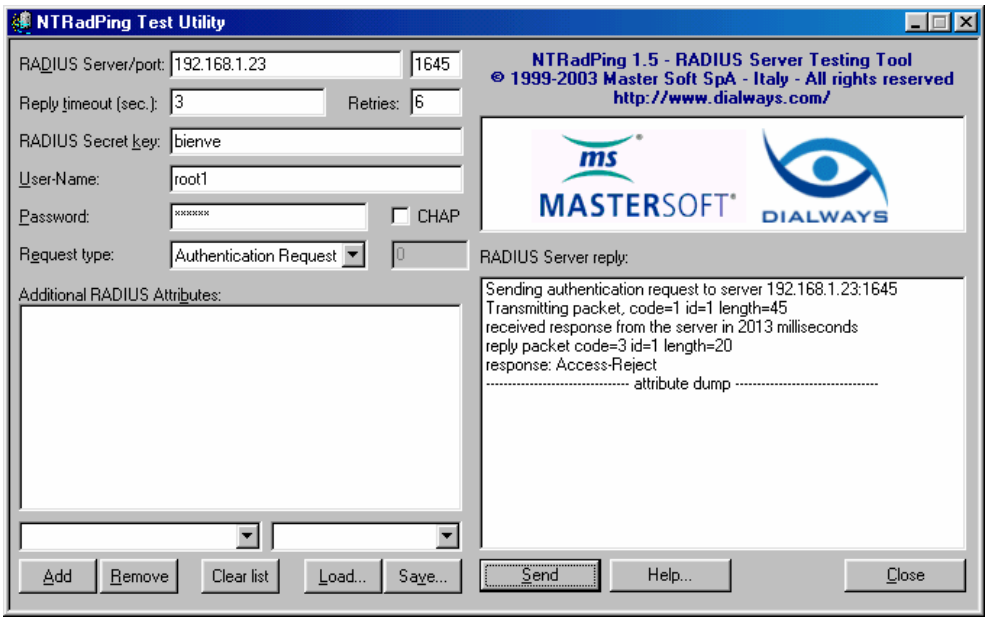

Figura –A.3- Fallo al realizar el *ping*

También puede darse el caso que haya un error en la conectividad de la red y el servidor RADIUS no pueda comunicarse con el cliente, en este caso el programa haría un número de reintentos igual al número indicado en la casilla *Retries* esperando un número de segundos en cada intento igual al indicado en la casilla *Reply timeout (sec)*. Esto puede apreciarse gráficamente en la figura 4:

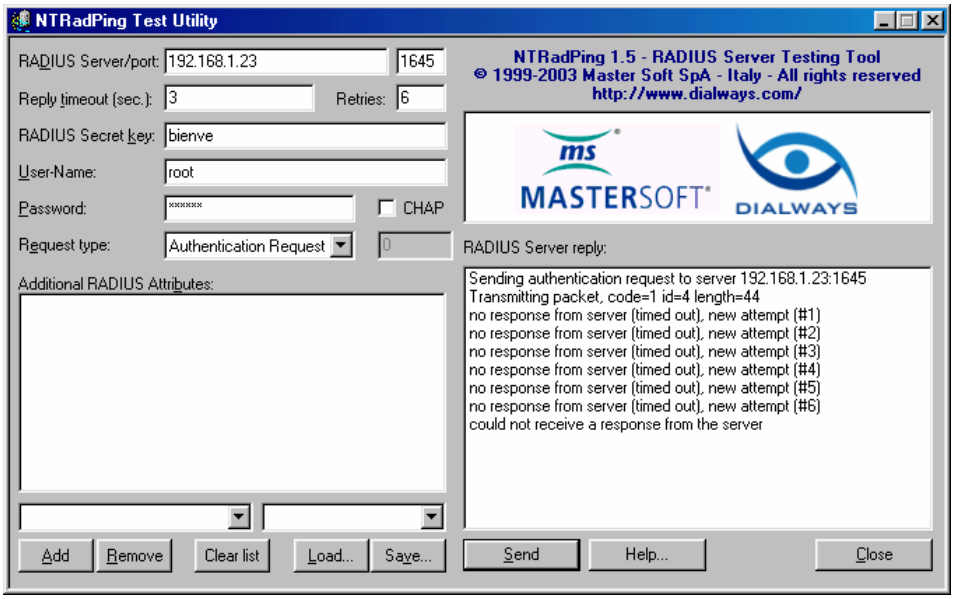

Figura –A.4- Mensaje de ausencia de respuesta desde el servidor

Una vez que todo ha funcionado correctamente, es decir, una vez que NTRadPing ha devuelto un *Acces-Accept* para el usuario *root* o cualquier otro usuario local de la máquina donde se está ejecutando el servidor RADIUS con su clave correspondiente, puede comenzar a hacerse uso del servidor RADIUS.

Apéndice B
Descripción del cliente EAP

Tal y como se especifica en el ejercicio propuesto, cualquier usuario que pertenezca a la universidad, antes de poder acceder a la red estará obligado a autenticarse en función de su indentificador de usuario y su clave. Por lo tanto, para que esto funcione es necesario instalar un cliente Odyssey (RADIUS) en todas las máquinas, que destaca por su amplia funcionalidad y facilidad de configuración. También podrían haberse usado otras posibilidades como por ejemplo el cliente EAP de Windows XP.

El *software* cliente puede descargarse desde la página de *Funk Software*. Una vez descargado se procede a su instalación mediante un sencillo *wizard*. Dentro de las opciones ofrecidas por el *software* nos interesa la opción *Odyssey Client Manager* desde donde se configura el cliente. El aspecto que presenta el *Odyssey Client Manager* al ejecutarse es el que se corresponde con la opción *Conection* en la que aparecerán las opciones relacionadas con la autenticación de la conexión.

Ventana Connection

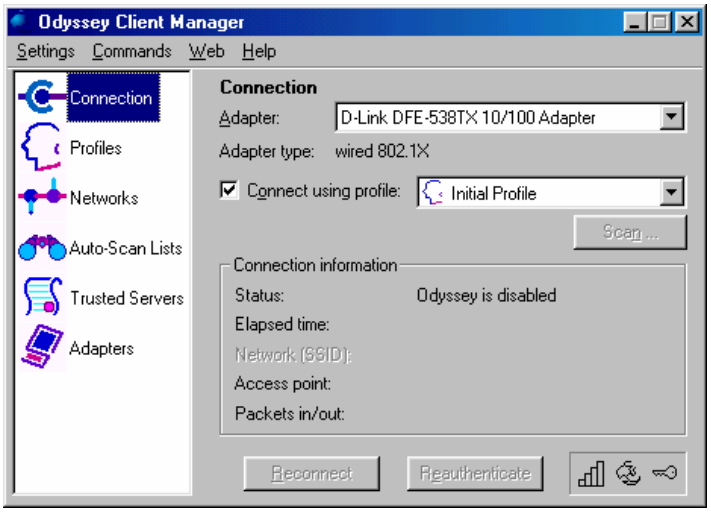

Figura –B.1- Ventana *Connection* del cliente *Odyssey*

En esta opción, se permiten configurar los siguientes parámetros relacionados con la conexión:

- *Adapter*: Se elige que adaptador de red de los que tiene instalada la máquina va a usarse para realizar la conexión.

  - *Adapter type*: Identifica el tipo de adaptador escogido para realizar la conexión, que puede ser cableado o inalámbrico

- *Conecting using profile*: Permite elegir el perfil de usuario con el que se quiere realizar la conexión. Más adelante se describe como crear dichos perfiles de usuario en el cliente Odyssey.

- *Connection information*: Cuadro en el que aparece un serie de información referente a la conexión:

- *Status*: Muestra el estado de la conexión, los valores más comunes que pueden observarse en este campo son:
  - *Open*: cuando la conexión está abierta.
  - *Authenticating*: cuando se está autenticando al usuario.
  - *Open and authenticated*: cuando la conexión está abierta y autenticada.
  - *Odyssey is disabled*: cuando el cliente está deshabilitado.

- *Elapsed time*: tiempo que lleva establecida la conexión.
- *Access point*: Punto de acceso que se está autenticando
- *Packets in/out*: Número de paquetes entrantes y salientes que atraviesan la conexión.

Ventana Profiles

Aquí se crean y editan los perfiles de usuario que luego podrán ser usados para establecer la conexión.

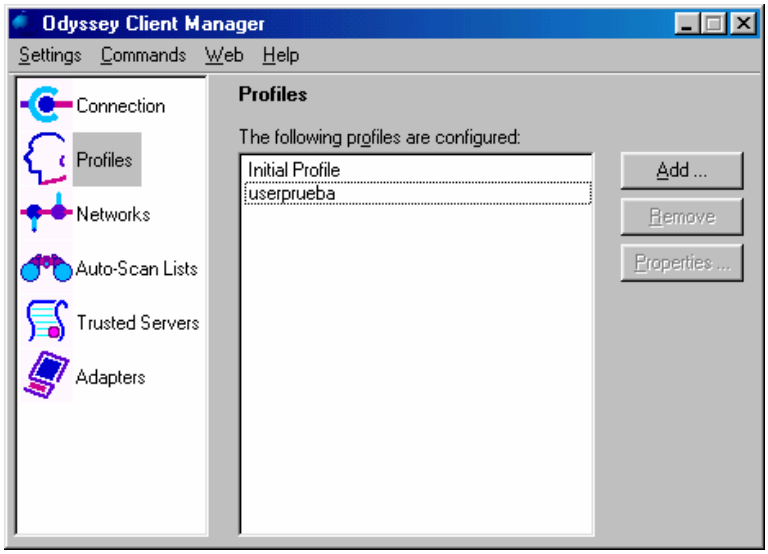

Figura –B.2- Ventana de *Profiles* del cliente *Odyssey*

Desde este cuadro de diálogo se pueden añadir o eliminar usuarios mediante los botones *Add* y *Remove*, o editar los perfiles de los usuarios ya creados.

Para crear un nuevo usuario se pulsa el botón *Add* accediendo de este modo a la la ventana de configuración de perfiles desde donde se configurarán los parámetros correspondientes al nuevo perfil que se desea crear.

Para modificar un perfil de usuario ya existente, basta con seleccionarlo de la lista de perfiles de usuario y pulsar el botón *Properties* accediendo de este modo a la ventana de configuración de perfiles desde donde se pueden modificar los parámetros correspondientes al perfil en cuestión.

Desde la ventana de configuración de perfiles pueden configurarse multitud de opciones de las cuales a continuación se describen las de mayor relevancia para la realización del ejercicio planteado. En primer lugar se encuentra el apartado *User_Info*, de este apartado para la realización del ejercicio se usarán los siguientes campos:

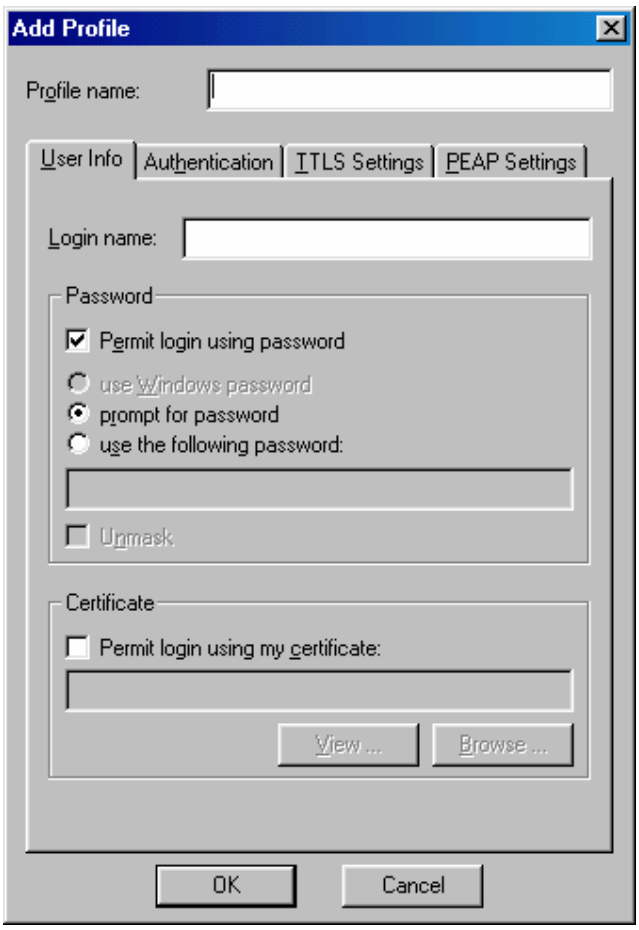

Figura –B.3- Ventana de información del usuario a crear

- *Login name*: campo donde se especificará el identificador de usuario.

- *Clave*: el cliente Odyssey permite configurar varias opciones relacionadas con la clave de usuario:
  - *Permit loging using Password*: casilla que se activa/ desactiva para permitir/no permitir el acceso usando una clave determinada.
  - *Prompt for password*: marcando esta opción el cliente muestra al usuario una ventana en la que éste debe introducir su clave para ser autenticado.
  - *Use the following password*: marcando esta opción se prescinde de la ventana de introducción de clave y se hace la autenticación mediante un clave especificado en la casilla inferior.

La siguiente pestaña que se encuentra el usuario es *Authentication*, en esta

Figura –B.4- Ventana de configuración del tipo de encriptación que usará un determinado usuario para el intercambio de mensajes del cliente *Odyssey*

ventana se elige el protocolo de autenticación que va a utilizarse para llevar a cabo la misma, pudiendo escoger entre:

- *EAP/TTLS*
- *EAP/PEAP*
- *EAP/T"OK"en Card*
- *EAP/MD5-Challenge*
- *EAP/LEAP*

Podemos elegir varios protocolos de autenticación los cuales se procesarán en orden descendente. El programa permite añadir y eliminar tantos como protocolos haya en la lista.

Las pestañas *TTLS Settings* y *PEAP Settings* son ventanas para configuración específica de determinados protocolos de autenticación que no van a ser usados para la resolución del ejercicio que se plantea en este proyecto.

Una vez configuradas las opciones deseadas se dota al perfil de un nombre mediante el campo *Profile name* se pulsa *"OK"* y el perfil de usuario queda añadido a la lista de perfiles de usuario o si hemos abierto un perfil para editarlo el perfil queda correctamente reconfigurado.

Ventana Networks

Desde aquí se decide para qué redes se configura el cliente Odyssey. Presenta las mismas opciones, en cuanto a lo que añadir, eliminar y editar redes se refiere, que la ventana *Profiles* para los perfiles de usuario. Desde la ventana *Networks properties* para la realización del ejercicio interesan las siguientes opciones de configuración:

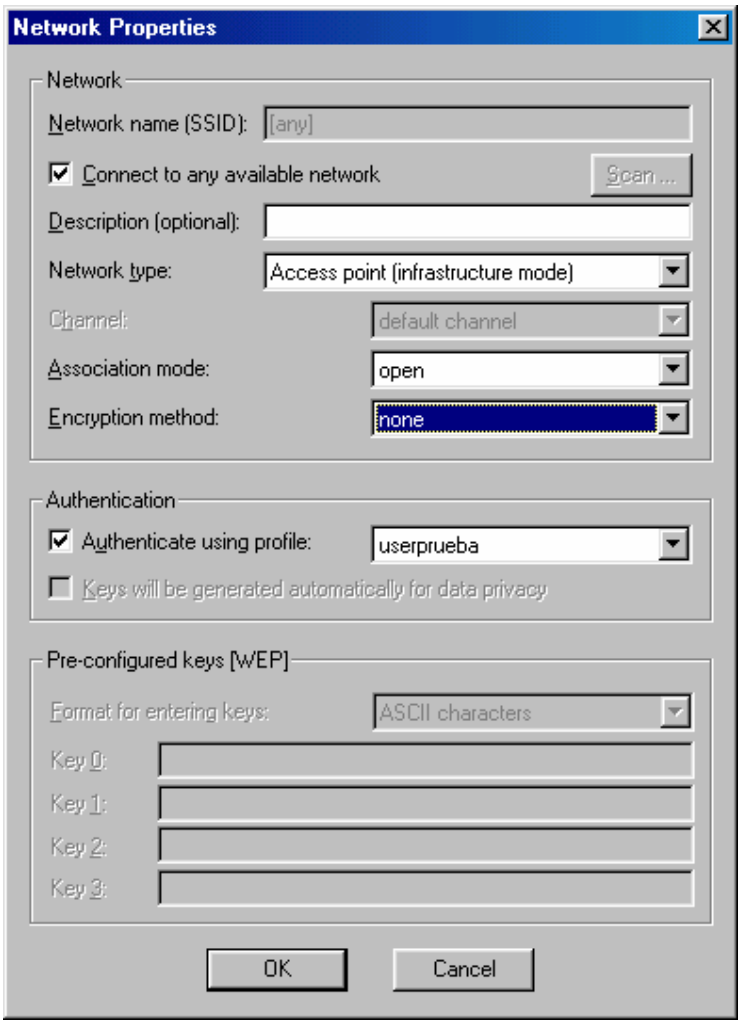

Figura –B.5- Ventana de configuración de las redes para las que se configurará el cliente EAP

- *Connect to any avaliable network*: esta casilla se activa/desactiva para posibilitar/no posibilitar la conexión a cualquier red disponible

- *Network type*: puede elegirse el tipo de red entre una red punto a punto, o una red inalámbrica.
- *Authentication*: dentro de este apartado interesa la casilla *Autenticate using profile* en la que se permite elegir el perfil de usuario mediante el que se va a autenticar el acceso a la red.

Ventana Adapters

La última ventana usada para el desarrollo del ejercicio es la ventana *Adapters* en la cual se muestra una lista de los adaptadores de red para los que está

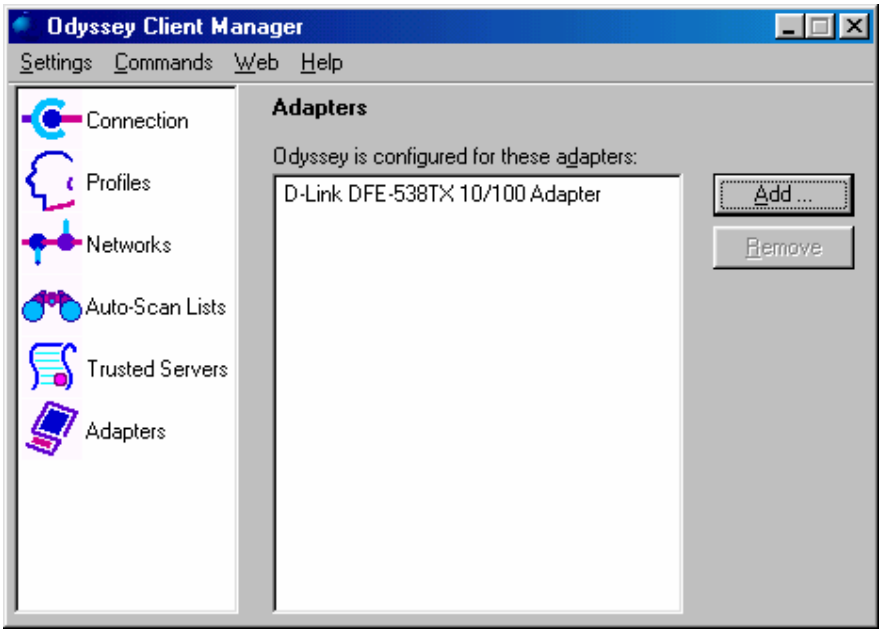

Figura –B.6- Ventana donde se configuraran los adaptadores del equipo para los que se utilizará el cliente *Odyssey*

configurado el cliente Odyssey. Puede añadirse o eliminarse adaptadores de la lista, pudiendo escoger entre adaptadores cableados o adaptadores inalámbricos mediante una sencilla ventana de selección. El programa de instalación detecta los automáticamente los interfaces de red instalados en el equipo durante la instalación del cliente Odyssey en el mismo.

Apéndice C
Servidor TFTP

El servidor presenta una interfaz gráfica muy sencilla y de las opciones que ofrece cabe destacar además de las relativas a la obtención de ayuda sobre el programa la opción *Configure* contenida dentro del menú *File* se pueden configurar los siguientes parámetros:

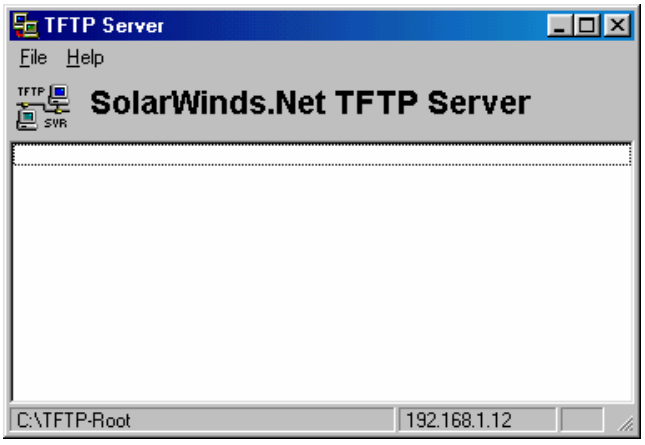

Figura –C.1- Interfaz del servidor TFTP

- TFTP Root Directory: El programa ofrece la posibilidad de elegir el directorio donde se guardan los ficheros que se mandan al servidor TFTP y desde donde se leen los ficheros demandados al servidor TFTP.

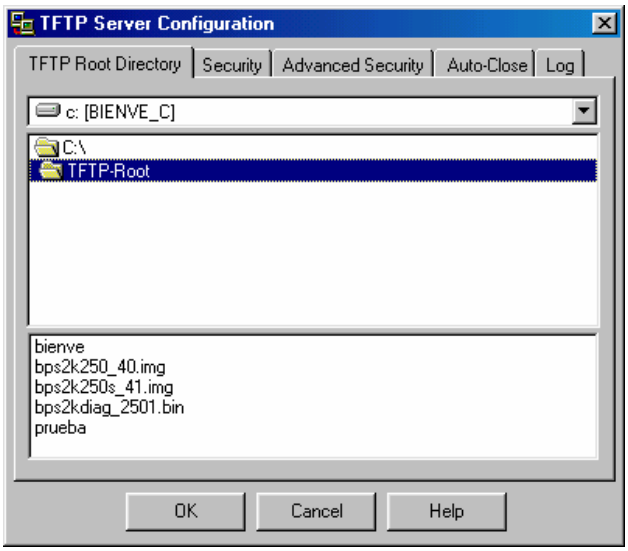

Figura –C.2- Ventana de configuración del directorio de intercambio de ficheros del servidor TFTP

- *Security*: Como opciones de seguridad básica puede configurarse únicamente si se permite o no el paso de:
    - Solamente paquetes recibidos.
    - Solamente paquetes enviados.
    - Tanto a paquetes enviados como a paquetes recibidos.

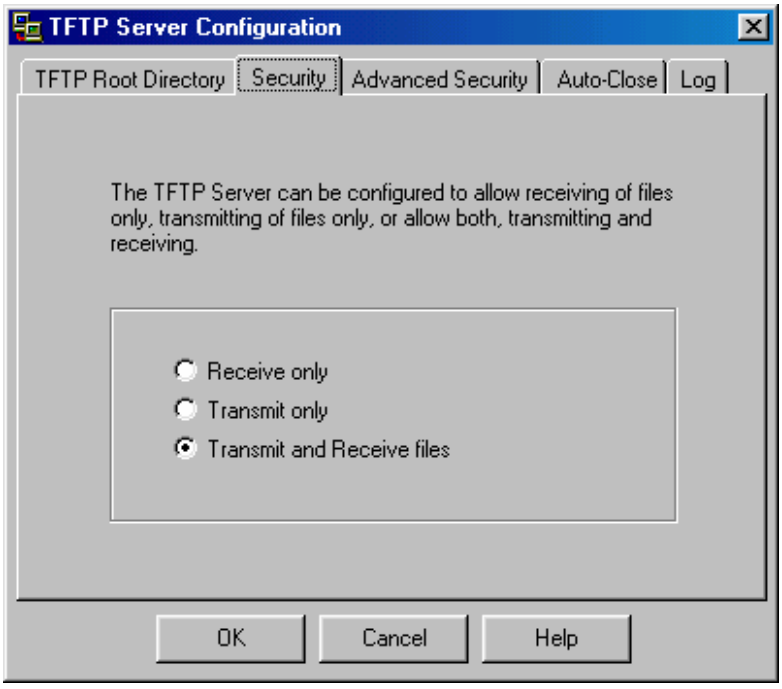

Figura –C.3- Configuración de la seguridad del servidor TFTP

- *Advanced Security*: Las opciones de seguridad avanzada se reducen a poder especificar un rango de direcciones IP que pueden actuar como clientes del servidor TFTP. La creación del rango de direcciones se realiza mediante una sencilla interfaz gráfica en la que se puede especificar la dirección inicio y fin de dicho rango. Una vez especificados ambos extremos, se añade el rango a la lista de rangos pulsando el botón *Add Range*. Para eliminar un determinado rango se selecciona éste de la lista de rangos y se pulsa el botón *Delete Selected Range*.

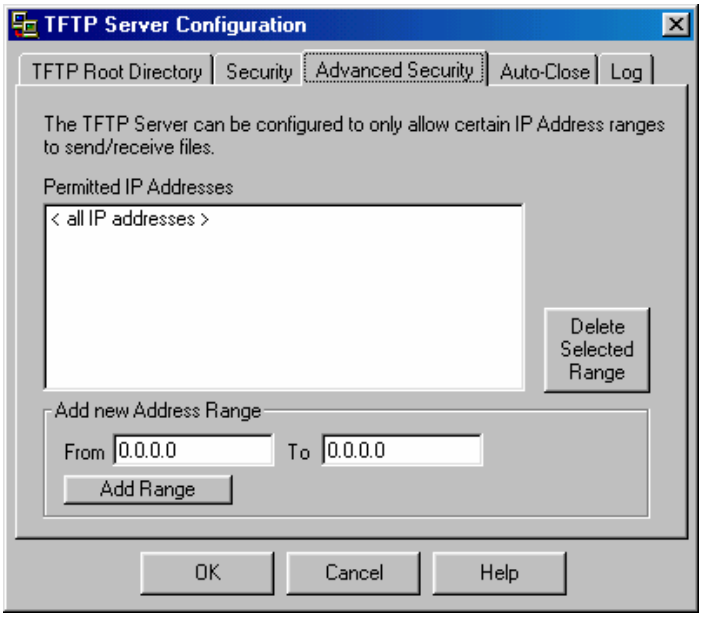

Figura –C.4- Interfaz de configuración de la seguridad avanzada para el servidor TFTP

- *Auto-Close*: Desde aquí puede configurarse el servidor para que se cierre de forma automática tras transcurrir un margen determinado de tiempo el cual puede elegirse de entre una serie de márgenes de tiempo que ofrece el programa, pudiendo elegir también la opción de no cerrarlo nunca, o lo que es lo mismo, mantener el servidor siempre activo.

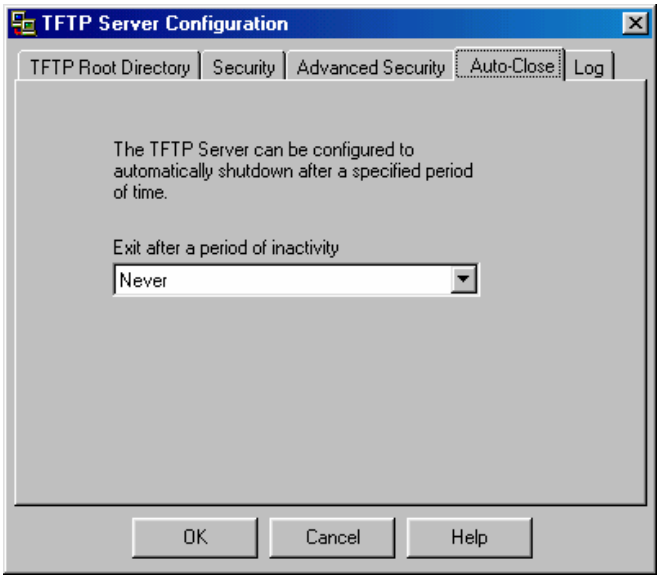

Figura –C.5- Interfaz de configuración de la desconexión automática del servidor TFTP

- *Log*: El programa permite también elegir si se quiere guardar un fichero de incidencias del servidor y, en caso afirmativo, especificar el directorio donde se guardan esos ficheros de incidencias.

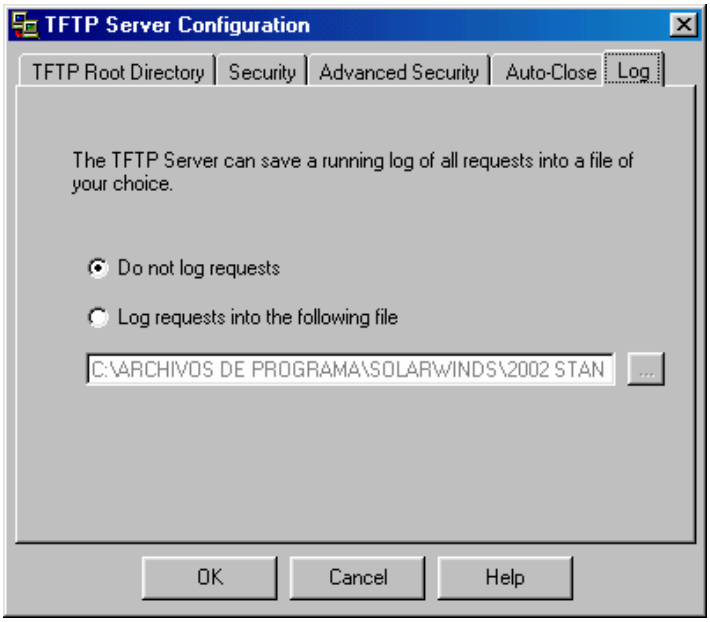

Figura –C.6- Interfaz de configuración de los archivos de incidencias

Bibliografía

[1] "*Practical Firewalls*" *by ferry William Ogletree*. Editorial: *Que*. *1st Edition* (12 Junio 2000). ASBN: 0789724162.

[2] "Sams Teach Yourself FreeBSD in 24 hours" by *Michael Urban*, *Brian Tiemann*. Editorial: *Sams*. Edición con libro y CD-ROM. ISBN: 0672324245.

[3] "RADIUS" *by Jonathan Hassell*. Editorial: *O´reilly&Associates, 1st Edition* (Octubre 2002). ISBN: 0596003226.

[4] http:// www.nortelnetworks.com

[5] "*Setting Up the Contivity 400 Unit*". *Nortel Networks* Julio 2001.

[6] "*Installing the Contivity Branch Access Management Software*". *Nortel Networks* Julio 2001.

[7] "*Using the Contivity Branch Access Management Software*". *Nortel Networks* Julio 2001.

[8] "*Reference for the Contivity Branch Access Command Line Interface*". *Nortel Networks* Julio 2001.

[9] "*Reference for the BPS 2000 Command Line Interface*". *Nortel Networks* Noviembre 2002.

[10] "*Using Web-based management for the BPS 2000 software*". *Nortel Networks* Noviembre 2002.

[11] "*Using the BPS 2000 software*". *Nortel Networks* Noviembre 2002.